

**DEPARTMENT OF HOMELAND SECURITY:
THE ROAD AHEAD**

HEARING

BEFORE THE

**COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE**

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JANUARY 26, 2005

Printed for the use of the
Committee on Homeland Security and Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE
20-169 PDF

WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska	JOSEPH I. LIEBERMAN, Connecticut
GEORGE V. VOINOVICH, Ohio	CARL LEVIN, Michigan
NORM COLEMAN, Minnesota	DANIEL K. AKAKA, Hawaii
TOM COBURN, Oklahoma	THOMAS R. CARPER, Delaware
LINCOLN D. CHAFEE, Rhode Island	MARK DAYTON, Minnesota
ROBERT F. BENNETT, Utah	FRANK LAUTENBERG, New Jersey
PETE V. DOMENICI, New Mexico	MARK PRYOR, Arkansas
JOHN W. WARNER, Virginia	

MICHAEL D. BOPP, *Staff Director and Chief Counsel*

DAVID KASS, *Chief Investigative Counsel*

JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Counsel*

MICHAEL ALEXANDER, *Minority Professional Staff Member*

AMY B. NEWHOUSE, *Chief Clerk*

C O N T E N T S

Opening statements:

	Page
Senator Collins	1
Senator Lieberman	4
Senator Akaka	7
Senator Domenici	9
Senator Pryor	10
Senator Warner	10
Senator Coburn	11
Senator Coleman	12
Senator Stevens	34

WITNESSES

WEDNESDAY, JANUARY 26, 2005

Richard L. Skinner, Acting Inspector General, Department of Homeland Security	13
James Jay Carafano, Ph.D., Senior Fellow, The Heritage Foundation	16
Michael Wermuth, Senior Policy Analyst, RAND Corporation	19
Stephen E. Flynn, Ph.D., Jeane J. Kirkpatrick Senior Fellow in National Security Studies, Council on Foreign Relations	23
Richard Falkenrath, Ph.D., Visiting Fellow, Foreign Policy Studies, The Brookings Institution	26

ALPHABETICAL LIST OF WITNESSES

Carafano, James Jay, Ph.D.:	
Testimony	16
Prepared statement	68
Falkenrath, Richard, Ph.D.:	
Testimony	26
Prepared statement	103
Flynn, Stephen E., Ph.D.:	
Testimony	23
Prepared statement	98
Skinner, Richard L.:	
Testimony	13
Prepared statement	51
Wermuth, Michael:	
Testimony	19
Prepared statement	79

APPENDIX

“Major Management Challenges Facing the Department of Homeland Security,” Office of Audits, OIG-05-06, December 2004, Office of Inspector General, Department of Homeland Security	118
“DHS 2.0: Rethinking the Department of Homeland Security,” SR-02, December 13, 2004, by James Jay Carafano, Ph.D., and David Heyman, The Heritage Foundation	143
“Evaluating the Security of the Global Containerized Supply Chain,” Technical Report by Henry H. Willis and David S. Ortiz, RAND	168
“Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat,” Occasional Paper by James Chow, James Chiesa, Paul Dreyer, Mel Eisman, Theodore W. Karasik, Joel Kvitky, Sherrill Lingel, David Ochmanek, and Chad Shirley, RAND	211

IV

	Page
Responses from Mr. Skinner to Post-hearing questions for the Record from:	
Senator Collins	267
Senator Akaka	272
Senator Coleman	282
Senator Lautenberg	285
Responses from Mr. Carafano to Post-hearing questions for the Record from:	
Senator Collins	294
Senator Coleman	297
Senator Akaka	305
Responses from Mr. Flynn to Post-hearing questions for the Record from:	
Senator Collins	309
Senator Coleman	312
Senator Lautenberg	316
Responses from Mr. Wermuth to Post-hearing questions for the Record from:	
Senator Collins	318
Senator Coleman	322
Responses from Mr. Falkenrath to Post-hearing questions for the Record from:	
Senator Collins	327
Senator Coleman	330

DEPARTMENT OF HOMELAND SECURITY: THE ROAD AHEAD

WEDNESDAY, JANUARY 26, 2005

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m., in room SD-342, Dirksen Senate Office Building, Hon. Susan M. Collins, Chairman of the Committee, presiding.

Present: Senators Collins, Lieberman, Stevens, Coleman, Coburn, Chafee, Domenici, Warner, Akaka, and Pryor.

OPENING STATEMENT OF CHAIRMAN COLLINS

Chairman COLLINS. The Committee will come to order. As I convene the Committee's first hearing of the 109th Congress, I want to express my appreciation to the Committee's Ranking Member, Senator Lieberman, who will be here shortly. I also want to express my appreciation to our other veteran Members for their commitment to the Committee's work and for choosing to return during this Congress.

The Committee also has four new Members: Senators Warner, Domenici, Chafee, and Coburn, and we look forward to working with them as well. Along with new Members, our Committee has a new name, Homeland Security and Governmental Affairs. While the new name will not win praise for its brevity or its style, it does reflect the Committee's expanded jurisdiction, and so it is appropriate that the Committee's first meeting of this year is an oversight hearing focusing on the Department of Homeland Security, evaluating the progress made so far and the challenges that remain.

As we prepare for the confirmation hearing of a new DHS Secretary, this assessment is especially timely. The title of our hearing today, "Department of Homeland Security: The Road Ahead," has a deeper meaning than might be immediately apparent. The Homeland Security Act of 2002 established a clear destination for the new Department. It was to prevent terrorist attacks within the United States, to reduce our vulnerability to terrorism, and to assist in recovery should an attack occur.

The precise route toward that destination, however, remains under construction. We are here to continue building a road that is as efficient, effective, and durable as possible. After the attacks of September 11, 2001, the security of America could not wait until this road was mapped out precisely and built to perfection.

The Department began operating under the constraints of a paradox. It had to meet immediately the new threat of the 21st Century with 20th Century components, all or part of some 22 existing Federal agencies with 180,000 employees, and it had to do so without neglecting the traditional missions of those agencies.

Any fair assessment will conclude that the Department under the leadership of Secretary Tom Ridge has made considerable progress. Our borders and transportation systems are more secure. Our critical infrastructure is better protected, and our emergency response capabilities are improved. But other reforms, such as the transportation worker identification credential, have lagged and it has been a daunting challenge for DHS leaders to integrate the 22 agencies while at the same time developing new policies that will make us safer.

The Homeland Security Act was not the last word on how we can best marshal our resources. As we proceed with this assessment, I am sure we will confront and I hope address the broad issue of better integration within the Department as well as a great many specific issues related to efficiency and effectiveness, accountability and authority.

Some observers may find it difficult to envision that a Department so large and with so many responsibilities could ever develop the efficiency, effectiveness, accountability, and durability to meet this challenge.

Yet, the Goldwater-Nichols Department of Defense Reorganization Act of 1986 proves otherwise. As a result of this act, the military's organizational culture has shifted dramatically over the last 20 years toward jointness and the combatant commands have produced far greater cohesion among the military services. I believe the Department of Homeland Security should strive for that same organizational culture and integration.

Today, we will hear from five witnesses, all of whom have scrutinized the Department. These witnesses will discuss several common problems that they have identified at DHS including a lack of strategic planning. Our witnesses today will discuss the Department's focus on managing daily crises and whether, as a result, it is not engaged in the necessary strategic planning.

Such planning is needed to ensure that we are directing the resources to the right places and that we are making the decisions today that will serve us well into the future.

Structural problems. Two years into the Department's life, we are now able to assess whether it is configured properly. The Heritage Foundation and CSIS have concluded that there are unnecessary layers of bureaucracy at DHS. They recommend, for example, the merger of two separate entities, the Customs and Border Protection, CBP, and the Immigration and Customs Enforcement, known as ICE, into "one unit with one uniform."

The need for clearer authorities. Some of our witnesses will discuss their belief that in a number of areas, there is a muddled division of responsibility between DHS and other agencies and departments. We will hear about the effects of such confusion as well as some possible solutions. These three problems and others our witnesses will discuss are obstacles in the road ahead and they must be cleared. I am particularly interested in the thoughts our wit-

nesses have on how these problems relate to several key areas of concern.

Border and transportation security were at the heart of the September 11 attacks. We were reminded of our vulnerability again just last week by what proved to be a false alarm in Boston regarding possible terrorists entering our country from Mexico.

In the hours and days after the September 11 attacks, we saw the vital role that emergency preparedness and response can play in reducing damage and loss of life. And we have done much to improve our capabilities at all levels of government since September 11. The identification of critical infrastructure and the hardening of targets or other forms of preparedness in which we have made some progress, but they remain a weakness in our homeland defense.

The Department of Homeland Security also plays an important role in our newly reorganized intelligence community. Because of the connections that it has already forged with our first responders, the Department is perhaps our strongest link with State and local authorities. This is an invaluable asset in intelligence that must be maximized. The integration of 22 agencies with thousands of employees in different cultures, practices, and areas of expertise into one cohesive entity remains a work in progress.

In fact, we were reminded just yesterday by the Government Accountability Office's list of high risk areas that this integration remains incomplete and information sharing among the Department's components and many other agencies and levels of government is inadequate.

We must improve department-wide management from procurement and contracting to information sharing and technology. We must eliminate unnecessary layers of bureaucracy and the barriers to communication that remain from the Department's creation. But we must do these things, always in the interest of reaching our destination with a minimum of detours.

Our witnesses today have studied the issues related to a stronger, more effective and efficient Department and a more secure homeland with great expertise and thoroughness, and I appreciate their joining us.

Finally, now that we have more Members present, let me say how proud I am of the very heritage and the record of this Committee. Our bipartisan collaboration and hard work last year produced landmark legislation, strengthening our intelligence community. It is my intention that we approach our work in the same spirit this year.

I am very fortunate to have an outstanding Ranking Member in that regard, and it is my pleasure now to recognize Senator Lieberman for his comments. I would note that we also are very pleased to have Senator Domenici returning to the Committee after a space of a couple of years and to welcome the distinguished Chairman of the Armed Services Committee, Senator Warner, who is joining the Committee, I believe, for the first time, and, of course, our stalwart Member, Senator Akaka, who plays such an important role, and it is wonderful to have you here today.

Let me also—I did it at the beginning of my comments—but welcome Senator Coburn for joining us and we have the distinguished

Member from Alaska, Senator Stevens, the Chairman of the Commerce Committee now, also joining us. I always like to recognize Senator Stevens because if he chose he could bump me as Chairman. [Laughter.]

So I am grateful that he has not chosen to exercise that prerogative and instead is chairing the Commerce Committee.

Senator Lieberman, welcome.

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. Thank you very much, Madam Chairman. Thank you for your kind words. I must say that working with you on this Committee has been one of the great pleasures of my 16 years in the U.S. Senate. You really set a standard for bipartisan leadership and I do think ultimately the Nation has benefitted from that and the work that we have done together. I look forward to this new session and continuing that work.

I also want to welcome the new Members of the Committee, those two promising rookies, Senators Warner and Domenici. [Laughter.]

It is like calling Roger Clemens a rookie. I only wish, John, that you were being compensated to the same level that Clemens is. [Laughter.]

It is quite a tribute to this Committee really that as you look around it we have Senator Stevens, Senator Domenici, Senator Warner, and on our side Senator Levin and Senator Carper. We have some real stature in the Senate. This may have become in some sense the Committee of Committees, but anyway I am honored by the two senior Members who have joined us and also particularly want to welcome Senator Coburn. It has been a pleasure to get to know you and I look forward to working with you.

Madam Chairman, as you well know, this is the first hearing of our newly named Committee, the Homeland Security and Governmental Affairs Committee, and it is quite appropriate that we are considering, as a matter of oversight, the state of our Homeland Security Department and looking at the road ahead.

We had substantial accomplishments over the last 3 years, and I think one of the most important tasks we can perform in these 2 years is to oversee the implementation of what we have started. Even before our jurisdiction was formally expanded in name, this Committee took the lead in restructuring our government post-September 11, to make our people safer.

We have had, I am proud to say, some historic and far-reaching successes. Last Congress obviously ended with the Intelligence Reform and Terrorism Prevention Act, remaking, we hope, an intelligence structure designed originally to fight the Cold War into one that is designed now to address the 21st Century challenges outlined by the 9/11 Commission.

Before the 9/11 Commission reported, we acted to address glaring weaknesses in our homeland defense revealed by the tragic events of September 11 by creating the Department of Homeland Security. Scores of Federal agencies had some responsibility for our homeland defense, but no single agency was clearly in charge. Our homeland defenses were disorganized because everyone was re-

sponsible but no one was accountable; the American people were left vulnerable.

Since its creation, the Department of Homeland Security has become the focal point in the fight against terrorism here at home and is now the place where citizens, State and local officials, first responders, and the private sector can look for leadership and resources in protecting the American people from terrorist attack.

But the Department of Homeland Security, which just celebrated its second birthday on January 23, is still obviously just a toddler. Those of us who worked to bring the Department into existence did not expect that the difficult job of creating a cohesive whole from so many different parts could be accomplished overnight or without some bumps.

This was, after all, the largest reorganization in our government in over half a century. We knew there would be significant challenges and difficult obstacles to overcome, but because the Department's mission is so vital to securing our Nation from attacks that are a clear and present danger, identifying and systematically removing those obstacles must be a top priority for the Administration and for Congress.

The Department has made real progress, but as we will hear today, there is much still left undone. And as a consequence, the American people remain simply not as safe as they should be. The absence of a well-designed strategy, a homeland security strategy, is one of the Department's most significant shortcomings. I was struck by the comment in the CSIS and Heritage report that Secretary Ridge was too often consumed by what was on his in-box, the immediate crisis of the day, understandable but troubling, because beyond the crisis of the day, this Department needs to stand up and defend us from the crisis of tomorrow.

The report's recommendation that a new Under Secretary, that is the CSIS and Heritage report recommendation that a new Under Secretary is needed to develop a homeland security policy and strategy for the longer term is, I think, a good one. It is critical that we have such a coherent plan so that our national priorities are known and everyone's responsibilities and roles are clear.

Encouraging news is that legislation we passed at the end of the last session requires the Department of Homeland Security to lay out its overall strategy as part of its long-term budgeting process. At the time this legislation passed, Senator Collins and I emphasized how important we thought it was to our homeland security efforts and what we expected to be included in the plan, and we will follow work on that plan very closely.

Second, DHS needs the most focused leadership and skilled management to address the shortcomings that we are going to hear about today from our witnesses. The Department must make certain that those officials responsible for integrating disparate systems and processes, the CIO, the CFO, and others, have sufficient authority to get the job done.

We cannot tolerate a Department where lines of authority do not align with responsibilities. From the reports that some of our witnesses will present today, that seems to be precisely and disconcertingly what we have in DHS. Nor can we tolerate a Department where the officials responsible for overseeing and managing

do not have adequate resources at their disposal to get the job done because if we give them authority but not resources to get the job done, we are still setting them up for failure.

And their failure, of course, is at our peril. Thus far, we simply have not made the necessary investments in homeland security. That is not just my conclusion, but a string of highly regarded, totally nonpartisan reports have agreed.

We have not invested enough in securing our ports or our rail systems, in defending our borders, or in preparing for bioterrorism attacks. Last year I proposed a budget that was \$14 billion above the Administration's budget to address these homeland security needs, and I honestly feel that every one of those dollars could have been spent in a way that was efficient and effective to our national homeland security.

In fact, there were some areas of homeland defense that actually had their appropriations and their allocations cut, and I know we are operating in a resource constrained environment, but we simply cannot go in this direction and expect that the people in DHS are going to do the job we want them to do.

Today, we are going to hear some proposals for reform. As we consider them, I want to note that the Intelligence and Terrorism Prevention law that was adopted last year, that the Chairman and I like to refer to as the Collins-Lieberman legislation, also contains some very significant measures to bolster our homeland security and will hopefully provide the Department and our government more tools with which to succeed.

I look forward to working with Members of this Committee and with the Administration to make sure that we faithfully implement these new provisions. Madam Chairman, again, thank you for convening this important hearing as the first of this session for this newly named and newly empowered Committee and for convincing so distinguished and experienced and knowledgeable a group of witnesses to come before us.

I look forward to working with you and other Members of the Committee and the Administration so that we can strengthen our Homeland Security Department, so that we can strengthen our homeland defense. I thank you very much.

Chairman COLLINS. Thank you. We have a quorum right now, and by January 31, we have to approve the Committee's funding resolution. So with the indulgence of our witnesses, I am going to interrupt the hearing very briefly to have a very brief business meeting so that we can do just one item of business, and that is to approve the Committee's funding resolution.

[Recess.]

Chairman COLLINS. We now return to the hearing, and I thank the indulgence of our witnesses. We need to have the money to keep going with these hearings. So thank you.

I have promised Members to have an opportunity for brief opening remarks today, but I would ask the Members to be very brief so that we can get to our witnesses. Senator Stevens.

Senator STEVENS. I merely wish to announce that the Commerce Committee will not hold a hearing on the nominee to be Secretary of Homeland Security. We will attend your meeting for that pur-

pose, and I urge Members to be brief also. We have a series of votes starting at 11:30.

Chairman COLLINS. Thank you. Senator Akaka.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Madam Chairman, I have some comments here and a statement. I ask that my full written statement be included in the hearing record.

Chairman COLLINS. Without objection.

Senator AKAKA. I wanted to say that I join you in welcoming the new Committee Members, now the Senate's lead panel on oversight of the Department of Homeland Security. I say this with pride because over the 15 years that I have served on our Committee, we have considered and Congress has enacted such landmark bills like the Chief Financial Officers Act, the Government Performance and Results Act, and the Clinger-Cohen Act, all of which I was proud to support. And our Committee enjoys a strong history of bipartisanship, inclusiveness and cooperation which I know will continue under your leadership and that of Senator Lieberman.

I have some concerns here that I will submit for the record that are very important, that have come about in the 2 years since the Department of Homeland Security was established. But I want to take time to thank Secretary Ridge, the outgoing Secretary of the Department, for his leadership during the agency's infancy. He undertook, as we know, an enormous and historic task, and I thank him for his service. And I think we can all agree there have been many successes under his leadership.

There is, however, much more room for growth which is the focus of today's hearing. And so I look forward to hearing our witnesses and want to place my full statement in the record.

Chairman COLLINS. Thank you very much, Senator.

[The prepared statement of Senator Akaka follows:]

PREPARED STATEMENT OF SENATOR AKAKA

Thank you, Chairman Collins. I join you in welcoming the new Members to our Committee, now the Senate's lead panel on the oversight of the Department of Homeland Security (DHS). I say this with pride because over the 15 years that I have served on our Committee, we have considered, and Congress has enacted, such landmark bills as the Chief Financial Officers Act, the Government Performance and Results Act, and the Clinger-Cohen Act, all of which I was proud to support. Our Committee enjoys a strong history of bipartisanship, inclusiveness, and cooperation, which I know will continue under the leadership of Chairman Collins and Ranking Member Lieberman.

Today we will review how well the Department of Homeland Security has defined and carried out its mission to protect the Nation. We must ask how well DHS has integrated the disparate cultures and management priorities of the 22 legacy agencies that were brought together under the most massive reorganization of the Federal Government since World War II. Before I go any further, I would be remiss if I did not thank Secretary Ridge, the outgoing secretary of the Department, for his leadership during the agency's infancy. He undertook an enormous and historic task, and I thank him for his service. I think we can all agree there have been many successes under his leadership. There is, however, still much room for growth, which is the focus of today's hearing.

Throughout the debate over the creation of DHS, I had four primary concerns. The first was the erosion of our constitutional freedoms through the collection, coordination, and storage of personal data. I am pleased that the Department has a strong privacy office in place and has replaced the proposed CAPPS II, a computer-assisted passenger pre-screening system which was widely criticized for a lack of privacy protection, with Secure Flight, which has more built in privacy safeguards.

Our Committee has also taken steps to improve coordination of activities between the Privacy Officer and the Officer for Civil Rights and Civil Liberties. However, the fact that the Department is reportedly operating, or planning to operate, 11 data mining activities that use personal information, troubles me. What are the safeguards in place to protect an individual's privacy rights? How is the Department ensuring the quality and accuracy of the information mined from the private sector? We must guarantee that the privacy of all Americans is protected as these activities are implemented.

The second issue was ensuring funding and support for the critical non-homeland security missions of those agencies merged into DHS, such as search and rescue, invasive species protection, and natural disaster emergency response. The unique multi-mission nature of these entities, such as the Coast Guard, the Federal Emergency Management Agency (FEMA), and the Animal and Plant Health Inspection Service, requires that special attention be paid to their non-homeland security functions. The hurricanes that slammed into Florida and surrounding States last year underscore the importance of FEMA's assistance to States and localities. To make certain that non-homeland security functions were not diminished, I introduced S. 910, the Non-Homeland Security Mission Performance Act, in April 2003. My bill required the Department of Homeland Security to identify and report to Congress on the resources, personnel, and capabilities used to perform non-homeland security functions, as well as the management strategy needed to carry out these missions. I will continue to monitor the critical non-homeland security responsibilities within the Department to ensure they are not shortchanged.

My third concern was how to protect the rights of the men and women who would staff the new Department because I feared that the new personnel authorities granted to DHS could erode worker protections. My initial fears were confirmed last year when DHS and the Office of Personnel Management (OPM) issued proposed regulations on the Department's new human resources system. This morning, DHS and OPM announced the final personnel regulations. While I am pleased that some of my recommendations to strengthen employee rights were included in the final regulations, I am afraid that changes to the proposed rules do not go far enough. The final regulations make dramatic changes in the way DHS hires, fires, classifies, and pays employees. The regulations call for the creation of an internal appeals panel for certain offenses, severely restrict the labor rights of employees, and tie the hands of the Merit Systems Protection Board to ensure that penalties for misconduct are just.

I look forward to working with my colleagues on the Committee and DHS to increase employee input, to provide opportunities for meaningful and independent oversight of labor and employee appeals, and to increase bargaining opportunities for employees. Together we can improve agency efficiency while protecting employee rights.

And lastly, I was concerned that the collective failure to respond to intelligence reports suggesting threats against America prior to September 11, 2001 was not being addressed.

Madam Chairman, I believe my fourth concern was addressed through the hard work of this Committee which successfully guided last year's intelligence reform bill through Congress. However, I do remain concerned about whether the true intent of our legislation will be realized in the execution phase.

There are a number of other management challenges that must be remedied for the Department to execute its many missions. For example, I remain deeply concerned about the budgetary and morale issues that plague Immigration and Customs Enforcement (ICE). ICE and Customs and Border Protection (CBP) personnel have expressed their concerns to me regarding the seemingly arbitrary manner in which the Immigration and Naturalization Service was split between ICE and CBP. The result has been mismanaged budgets, which prompted a hiring freeze for ICE and CBP in the spring of 2004; an ongoing overall budget freeze for ICE; and low staff morale.

The ICE agents also consider themselves disadvantaged because they have been separated from their former colleagues at CBP with whom they developed collaboration. The Center for Strategic and International Studies-Heritage Foundation Report, "DHS 2.0," recommends merging the two entities. I will review this proposal carefully because the Border and Transportation Security Directorate must eliminate the existing barriers to be an effective guardian of our Nation's borders.

Attention must also be given to the disjointed manner in which international affairs is handled in DHS. The Office of International Affairs (OIA), which was created and placed in the Office of the Secretary by the Homeland Security Act, failed to live up to its intended vision for a number of reasons, not the least of which is funding. The OIA has an annual budget of approximately \$1 million and a staff of

10, the majority of whom are detailees. These resources are inadequate for an office expected to promote information sharing, organize training exercises, plan conferences, and manage the international activities of DHS. As a result, much of the international coordination has been left to the individual directorates which sends a disjointed message to the international community.

International cooperation, whether it is in the area of cargo security or the prevention of illegal immigration, is crucial to the security of the United States. Having the appropriate structure in place in the Department to facilitate and foster that cooperation should not be overlooked.

We in the Congress often speak of an agency's success in terms of funding levels and overarching policy. These issues are important. But I submit that internal structural, financial management, and personnel concerns matter just as much, if not more, in the effectiveness of an entity as mammoth as DHS. I hope we can use today's hearing as an opportunity to explore how to improve DHS in these critical areas. I thank our witnesses for being here with us today, and I look forward to your testimony.

Chairman COLLINS. Usually we follow the early-bird rule, but today I am just going to go in order of seniority. Senator Domenici.

OPENING STATEMENT OF SENATOR DOMENICI

Senator DOMENICI. I will be very brief. Actually I did not read your analysis or your testimony, but I think the biggest problem we have is not the problem of what we are not doing, but what we are doing, because I believe there is a significant lack of risk prioritization. We cannot cover every risk that people dream up. If we did, we would spend more on this than the defense of our Nation, and we would give everybody what they want. Every small fire department across the country would want new fire trucks because they are part of homeland security, and that is not disparaging of the fire departments. There are many other groups just like them.

I am very worried that this process could lead to the funding for homeland security to be the most recent piggy-bank, Christmas tree, whatever you want to call it, for congressional wish lists. And I do not know what this Committee can do about it because it is principally an appropriations item. But when the good senator, Senator Lieberman, said we have to do more, and then he talked about making sure that things did not get in here by ships and trains and the like, I believe, we cannot do all of that and do all the other things we are asking to be done with this funding.

I do not know, Mr. Wermuth, if you addressed that issue. Did you?

Mr. WERMUTH. I did, sir.

Senator DOMENICI. I think this issue is really paramount because 2 or 3 years from now people may look back and say, we thought we were doing homeland security, but essentially we did not address a big need because we were doing so many things we should not have been doing. Every city in America is not under risk of attack by terrorists. They might think they are; they might be worried about it. But somebody has to determine which, why and what for every item that we fund.

Madam Chairman, I believe that you and the Ranking Member have a very serious responsibility in this regard. Everybody is going to be asking you to put every type of project in homeland security. I regret to say it is very hard to turn people down, but the truth of the matter is we cannot be a risk-free America. Something has to be at risk or we just cannot afford homeland security.

I thank you for giving me time.

Chairman COLLINS. Thank you. Senator Pryor, we are delighted to have you back.

Senator PRYOR. Thank you.

Chairman COLLINS. I know given your seniority on the Committee and the change in ratios that you had to work to remain on the Committee and we are very happy that you did.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Thank you so much. And thank you, Madam Chairman. I look forward to working with you over the next 2 years, Senator Lieberman and the entire Committee, including our new Members here, but I look forward to hearing from the panel today and hope we will focus on making America more secure in a very real and meaningful way. I would like to get your thoughts and insights on that. Thank you. And I have a statement for the record.

Chairman COLLINS. All statements will be entered into the record as if read.

[The prepared statement of Senator Pryor follows:]

OPENING PREPARED STATEMENT OF SENATOR PRYOR

Thank you Madam Chairman and Senator Lieberman for convening this hearing. I would also like to thank the witnesses who are testifying here today for providing their expertise and insight as we look at some of the challenges at DHS over the last couple of years as well as the potential changes to be made in order to address those challenges.

As the 9/11 Commission discussed in its report, since its creation in 2002, DHS has had the “lead responsibility for problems that feature so prominently in the September 11 story, such as protecting borders, securing transportation and other parts of our critical infrastructure, organizing emergency assistance, and working with the private sector to assess vulnerabilities.” (9/11 Report, p. 395) Such responsibility is monumental.

We are here today to review the challenges and opportunities at DHS. Our Committee has worked together in its commitment to making our country safer. We most recently, guided by the leadership and tenacity of Madam Chairman and our Ranking Member, worked in a bipartisan manner to evaluate and implement the recommendations of the 9/11 Commission, which resulted in the recent passage of the Intelligence Reform and Terrorism Prevention Act.

Today we are here, guided by that same commitment as we consider and address the development of DHS.

Chairman COLLINS. Senator Warner.

OPENING STATEMENT OF SENATOR WARNER

Senator WARNER. Madam Chairman and the Ranking Member, I thank you for the opportunity of serving with both of you. We have had long associations on the Armed Services Committee, and I view the work of this Committee as being parallel in many respects to the overall responsibility to protect our Nation, and I think that I can work with you in carefully following the existing law with regard to the separation between the powers of the military abroad and the powers to take and exercise in the continental limits, but we have got to have a seamless concept of protecting this country.

Also, I was privileged to be a member of the Armed Services Committee working with Senator Goldwater when Goldwater-Nichols was drawn up. It took us a year to really finalize that very vital

piece of law. It has proven its value, and I think it was important that you used that as a benchmark today.

So I thank you. And lastly, I do not know that I can depart without saying what a magnificent chair this is as compared to the wooden benches we use in the Armed Services Committee.

Chairman COLLINS. Just another advantage of this Committee. [Laughter.]

Senator WARNER. A very distinct advantage.

Senator LIEBERMAN. I do want to say, Senator Warner, that this is a legacy of the Fred Thompson Administration. [Laughter.]

Chairman COLLINS. Senator Coburn.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Well, I just wanted to thank you for the opportunity to serve with each and every Member of this Committee. I do have a statement for the record, and ask unanimous consent that it be in the record.

Chairman COLLINS. Without objection. Thank you.

[The prepared statement of Senator Coburn follows:]

PREPARED STATEMENT OF SENATOR COBURN

Thank you Chairman Collins. I am pleased to join you as one of the newest Members of the Homeland Security and Governmental Affairs Committee. I look forward to working with you and Members of this Committee on rigorous oversight of the Department of Homeland Security and other Federal programs, as well as on initiatives that will reduce and eliminate wasteful government spending.

I commend your leadership, Chairman Collins, for holding this hearing on the future direction of the Department of Homeland Security as the Committee's first hearing of the 109th Congress. As this Department—with approximately 190,000 employees and a budget of over \$33 billion—enters its third year with new leadership, it is fitting that this Committee examine the current status of the Department's operations and proposals to increase its effectiveness.

One such proposal entitled, "DHS 2.0: Rethinking the Department of Homeland Security," was issued jointly last month by the Heritage Foundation and the Center for Strategic and International Studies. I look forward to hearing today from Dr. Carafano, a co-author of the report, on his call for a full assessment of the Department's organizational structure to improve efficiency and to prevent existing homeland security grant programs from turning into another Federal pork barrel program.

In addition, the Department's Office of Inspector General, from which we will also hear today, issued a report last month on major management challenges facing the Department. Some of these challenges include the potential for overlapping grant funding, inadequate staffing for program administration, structural problems in the Department's financial management organization, and deficiencies in the Department's IT organizational structure.

Yesterday, the Government Accountability Office (GAO) issued its biennial assessment of Federal programs, and again for the second consecutive time, listed the Department of Homeland Security on its "High Risk List." The GAO recognized the steps the Department has taken over the past 2 years, but is concerned whether the Department will follow through on its initial efforts, whether the Department has made enough progress in forming partnerships with governmental and private sector entities, and whether the Department has sustained leadership to complete the transformation.

It is clear that much work needs to be done to improve the organization structure, reduce bureaucratic overlap, and strengthen the financial accountability of the Department of Homeland Security. I look forward to hearing the recommendations from our witnesses to address these issues.

Thank you, Chairman Collins.

Chairman COLLINS. Senator Chafee, you were not present when I welcomed you to the Committee so let me do so again now. We are delighted to have you as a Member.

Senator CHAFEE. I look forward to serving with you and look forward to the witnesses' testimony on this important subject. Thank you.

Chairman COLLINS. Thank you. Senator Coleman.

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. Thank you. It is great to be back. I appreciate your great leadership and appreciate, as the new Members will see, the incredible strength of the bipartisan relationship on this Committee with great respect for the work of the Ranking Member also. So it is a pleasure to be here and I look forward to the testimony, Madam Chairman. Thank you.

[The prepared statement of Senator Coleman follows:]

PREPARED STATEMENT OF SENATOR COLEMAN

Madam Chairman, I want to thank you for holding this important hearing on the future of the Department of Homeland Security. I want to join in thanking all the members on the panel for appearing this morning before the Committee to discuss what lies ahead on this important issue.

My home State of Minnesota has a wide range of Homeland Security interests given that we share an international border with Canada, we have two major cities in Minneapolis and St. Paul and we have a major port in the city of Duluth. Unfortunately, however, this year Minnesota witnessed an average 48 percent reduction in the allocation of Federal homeland security dollars, including a 71 percent reduction to our urban area security initiative alone. As the Department of Homeland Security evolves, Members on this Committee will have to provide effective oversight to ensure that policies and strategies pursued are well thought out and provide the best security possible.

On that note, the Permanent Subcommittee on Investigations is currently pursuing three areas of oversight regarding the response of the Department of Homeland Security to the threat of nuclear terrorism: The Container Security Initiative, the Customs Trade Partnership Against Terrorism and the deployment of radiation portal monitors. I am also interested in ways we can remove unnecessary bureaucratic hurdles for students wishing to study in the United States and reverse the perceptions about America being unwelcome to foreign students.

I am very interested to hear the panelist's thoughts on these issues and their feelings on the long term development of the Department of Homeland Security.

Chairman COLLINS. Thank you. You have been one of our most active Members and we are delighted to have you back as well. Thank you.

I would now like to turn to our patient witnesses. Our first witness today is Richard L. Skinner, the Acting Inspector General at the Department of Homeland Security. Mr. Skinner will discuss the report issued last month by his office on the management challenges facing DHS.

Next, we will hear from James Carafano, a Senior Research Fellow at the Heritage Foundation in Defense and Homeland Security. Dr. Carafano is the co-author of the study that we will be discussing today.

Following him will be Michael Wermuth, a Senior Policy Advisor Analyst in Domestic Terrorism at the RAND Corporation. I had the pleasure of having dinner recently with Mr. Wermuth in Los Angeles and I was so impressed with the work that RAND had done that I asked him to join us today.

Stephen Flynn is not new to this Committee. He has been an expert witness for us before and we are delighted to have him back. He is the Jeanne J. Kirkpatrick Senior Fellow for National Security Studies at the Council on Foreign Relations. He is also a retired

Coast Guard Commander and a foremost expert on transportation and border security.

Last, but certainly not least, we will hear from Richard Falkenrath, a Visiting Fellow in Foreign Policy Studies at The Brookings Institution. His background includes serving as Deputy Homeland Security Advisor to the President and as Senior Director for Policy at the Office of Homeland Security.

I welcome all of you. I appreciate your being here. Mr. Skinner, we will start with you.

**TESTIMONY OF RICHARD L. SKINNER,¹ ACTING INSPECTOR
GENERAL, DEPARTMENT OF HOMELAND SECURITY**

Mr. SKINNER. Good morning, Madam Chairman, Ranking Member Lieberman, and Members of the Committee. Thank you for the opportunity to be here today especially with such a distinguished panel. I have submitted a written statement for the record. If I may, I could just summarize that statement in my remarks here today.

Chairman COLLINS. Please do so.

Mr. SKINNER. First, however, if I can take this opportunity, I would like to commend Dr. Carafano and the Heritage Foundation for the outstanding report, "Rethinking Department of Homeland Security." While we may not be able to address each and all those recommendations in that report, you can be sure that we will consider that report and use it as a guidepost as we plan our work in the future.

Over the past 2 years, I have personally visited with departmental employees at our land ports of entry, at our seaports, airports, detention facilities, enforcement offices, Coast Guard facilities, and in our disaster field offices. I can assure you that at each and every site that I visited I found dedicated, hardworking employees who are genuinely committed to securing this country or servicing those affected by disasters and making the Department a model for the entire Federal Government.

There is no question that the Department has made great strides toward improving homeland security. No one here today can deny that our Nation is more secure today than it was 2 years ago. That said, the Department still has much to do before it can be called a cohesive, efficient, and effective organization.

It will not be easy and it cannot be done in 1, 2 or 3 years. GAO has noted that successful transformations of large organizations under even less complicated situations could take from 5 to 7 years. The Committee has asked me to focus on challenges related to border and transportation security, integration, intelligence, and preparedness.

I would like to highlight the significant issues that we have reported on in the past 2 years. First, I would like to talk about border security. Our Nation's homeland security does not stop at our geographic borders. Programs to promote international travel create potential security vulnerabilities that may allow terrorists, criminals, or other undesirables to enter this country undetected.

¹The prepared statement of Mr. Skinner appears in the Appendix on page 51.

For example, the Department must address security concerns identified in the Visa Waiver Program. The Visa Waiver Program enables citizens from 27 countries to travel in the United States for tourism or business for 90 days or less without obtaining a visa. These travelers are inspected at a U.S. port of entry but have not undergone the more rigorous background investigations associated with visa applications.

Also, the Department continues to experience problems in identifying and detecting aliens presenting lost or stolen passports from visa waiver countries. Procedural shortcomings permitted some aliens presenting stolen passports to enter the United States even after the stolen passports were detected.

Information on lost and stolen passports provided by visa waiver governments was not routinely checked against U.S. entry and exit information to determine whether stolen passports had been used to enter the United States.

In addition, there was no formal protocol for providing information concerning the use of stolen passports to the Department's Office of Immigration and Customs Enforcement.

Further, the Department also must address issues with its visa security program, which stations officers at U.S. embassies and consular offices overseas to review visa applications and perform other law enforcement functions. The Department used temporary duty officers who often did not have the required background or training including language training or skills to perform effectively as visa security officers.

With respect to international travels, two major border security challenges confront the Department and that is, one, the diversity in the biometric system used to identify travelers and, two, the disparity in the level of scrutiny given to the different types or classes of travelers entering the United States.

With respect to terrorist weapons, one of the primary responsibilities of the Department's Office of Customs and Border Patrol is to detect and prevent terrorist weapons from entering the United States. This includes ensuring that oceangoing cargo containers arriving at our seaports are not used to smuggle illegal contraband.

As you may recall, *ABC News* was successful in two attempts at smuggling depleted uranium into the country. In a September 2004 classified report, we cited several weaknesses that occurred at the time of the two incidents that made the container protection inspection process less effective. We are now following up to ensure that the Department has taken corrective actions.

With regards to transportation security, the success of the Transportation Security Administration, that is TSA, depends heavily on the quality of its staff and the capability and reliability of equipment to screen passengers and cargo while at the same time minimizing disruption to public mobility and commerce.

Our undercover audits of screener performance reveal that improvements are needed in the screening process to ensure that prohibited items are not being carried onto airplanes or do not enter the checked baggage system. We plan to complete another round of undercover tests. We should have that review completed within the next 2 months.

While TSA continues to address critical aviation security needs, it is moving slowly to improve security across other modes of transportation. About 6,000 agencies provide transit services through buses, subways, ferries, and light rail service to about 14 million Americans daily. The terrorist experiences in Madrid and Tokyo highlight potential vulnerabilities in our transit systems.

Although it is currently coordinating the development of a national transportation sector plan, which is expected to be completed later this year, TSA's 2005 budget still focuses its resources on aviation.

Also, the Coast Guard's willingness to work hard and long hours, use innovative tactics and work through interagency partnerships has allowed it to achieve its performance goals. However, to improve and sustain this mission performance in the future, the Coast Guard faces significant barriers, most importantly the deteriorating readiness of its fleet assets.

Finally, with regard to integration and preparedness, we reported that structural and resource problems continue to inhibit progress in certain support functions. For example, while the Department is trying to create integrated and streamlined support service functions, most of the critical support personnel are distributed throughout the Department's components and are not directly attributable to the functional chiefs. That is, the Chief Financial Officer, the Chief Information Officer, and the Chief Procurement Officer.

The Deputy has structured the functions based on a concept of dual accountability where both the operational leadership and the functional chiefs are responsible for the preparation of operational directives and their ensuing implementation. This concept has been described as a robust dotted line relationship.

While the concept may be workable in some environments, we have concerns that within the Department the functional chiefs may not have sufficient resources or authority to ensure that Department-wide goals are addressed in an effective, efficient or economical manner or that available resources can be marshalled to address emerging problems.

Furthermore, on the program side of the house, the Department's Information Analysis and Infrastructure Protection directorate, or IAIP, which has primary responsibility for critical asset identification, prioritization and protection has yet to produce a condensed list of most sensitive critical assets.

Consequently, other elements within the Department are at risk of failing to direct their scarce resources toward national critical infrastructure protection and preparedness priorities. For example, in its Port Security Grant Program, the Department awarded three rounds of grants totaling \$560 million without definitive national priorities for securing the seaport infrastructure of the Nation.

Poor integration of critical asset information with the Department's Protection and Preparedness Initiatives meant that the port security grants were awarded without sufficient information about our national seaport priorities.

Department components need to integrate better their decision-making processes with the infrastructure protection component of the Department's IAIP directorate.

Regarding preparedness, I would like to comment briefly on the Heritage Foundation's recommendations to consolidate the Department's preparedness function under an Under Secretary for Protection Preparedness. Based on my own experiences while I was Acting Inspector General at FEMA and the Deputy Inspector General at FEMA from 1991 to 2003, I have reservations about segregating FEMA's preparedness function from its response and recovery responsibilities.

Disaster response, preparedness response, and recovery are integrally related, each relying on the other for success. The proposal should be studied very carefully before it is put into practice.

Madam Chairman, this concludes my remarks. I will be happy to answer any questions you or Members of the Committee may have.

Chairman COLLINS. Thank you. Dr. Carafano.

TESTIMONY OF JAMES JAY CARAFANO, PH.D.¹ SENIOR FELLOW, THE HERITAGE FOUNDATION

Mr. CARAFANO. Thank you, Madam Chairman. I would like to commend the Committee for having these very important hearings and for its leadership on either the Lieberman-Collins bill, or the Collins-Lieberman bill, or the intelligence reform bill, but I mean your leadership was outstanding, and we certainly would not have had the legislation that we did without your leadership.

I have submitted a statement for the record, and I would just like to briefly cover three points. I will talk briefly about the report, three of the major recommendations, and then a suggestion of a way ahead that the Congress and Department might consider.

This began really with my prejudice both as a historian and 25 years in the Army, about a dozen of those working in and around the Pentagon. And the lesson, when what became the Department of Defense was created in 1947, there were fundamental things in its structure and organization that prevented the effective coordination between the services and oversight of the services.

Eisenhower talked about them as Chief. He talked about them as Acting Chairman. He talked about them as President. They simply did not get fixed and you are absolutely right. They did finally get fixed in the Goldwater-Nichols Act of 1986, a mere 3 years before the end of the Cold War. And I think quite honestly the lesson we can learn is we can do much better.

We can recognize the operational challenges that have presented themselves since the Department was created and fix them now. With that, the Center for Strategic International Study and the Heritage Foundation put together a team of about 30 young professionals, which I define as anybody under 50, who did a terrific job looking at—we tasked them in four different areas: Management, resources, authority, and roles and missions. And they produced a report that had about 40 recommendations, and we could debate the merits of each of the recommendations, but I think on the whole what they represent is a pretty substantive argument that it is worthwhile to go back and rethink the fundamental structure of the Department and its roles and missions and fix obvious

¹The prepared statement of Mr. Carafano appears in the Appendix on page 68.

things now before they become stovepipes and stakeholders take hold and it just becomes too hard to do.

Reviewing the report, in retrospect, three principles evolved for me in terms of to guide further reform, and I would just like to cover those very quickly and illustrate them with an example of each.

The first one is do management first. I mean the IG report which came out very close to ours, I thought, was very instructive. It talked about a number of programmatic issues, but I think at the root of all of those were a cleaner management structure, clear responsibilities, the ability to establish priorities and set authorities would be the first step in addressing many of these challenges. And I think one good example of that is policy. The Department, and our recommendation was, simply needs an Under Secretary for Policy.

This is no more clearly illustrated than in international affairs. I mean right now there are arguably two centers of gravity. There is an Office of International Affairs. There is a policy advisor to the Secretary. They are competing to make policy and all the subordinate agencies who have international affairs, basically they get a choice. They can go to whoever they like who has the right answer. And you do not have an international affairs policy that is coherent across the Department.

That particularly reflects badly in the Department's dealings with other agencies and in international forums. It does not have the gravitas. It does not have the long-term experience. It does not have the cohesive position of the Department behind it to really work well in these environments.

The second guiding principle that I really call is envisioning the future and there is lots of debate about do we have the roles and missions exactly right; do we have the split exactly right? And how do you really determine that? And I think the right answer to the question is you have to decide where you want to be in 5 years? What do you really want this function to be doing? And if you could make that strategic decision, then the answer is what the organization ought to look like ought to be pretty clear.

Now, one of our probably most controversial recommendations is to merge the Customs and Border Protection and Immigrations and Customs Enforcement into a single agency. That was really based on two observations. One is we could not find a good argument for splitting them, and what you are intentionally doing is creating opportunities for disconnects and gaps between investigative operations and ongoing operations in one and the other. And why are you creating a need for coordination when you do not need one?

And the second one is—is really the management challenge—is in ICE and CBP. You know, ICE, for example, when INS would split, it was the budget of INS was basically split among three different functions. That has created an enormous budgetary challenge and we all know that ICE had enormous financial challenges. I think the last figures I saw were upwards of \$300 million, to the point that operations simply cannot be conducted at the end of the year. People cannot use credit cards. People cannot go on travel. Hiring freezes. Now, is that the right answer? Well, quite honestly, I do not know if merging CBP and ICE will solve a lot of these

problems or if that is the best way to solve these problems or if there are other solutions.

But I do think that the right answer is to sit back and strategically ask what do we want border and internal enforcement security to do—how do we want that done 5 years from now? And if we can decide that, then I think the organizational answer ought to present itself.

And the third point or principle I would argue for is the clear division of responsibilities between operators and supporters, and I think here the DOD model, Defense model serves very well. I mean in Defense we have warfighters. We have combatant commanders whose job it is to go out there everyday and find the bad guy and get rid of him.

And then we have services which are basically force providers. It is their job to provide trained and ready forces for the warfighter. I think that model has a lot of merit to it, and I think there are many areas where it could be applied within DHS.

Preparedness and response, I think, is one of them. Response is clearly an operational function. You want the guy who is in charge of response to be ready to respond, to be thinking about responding, and have that be the sole focus of the organization's mission.

Preparedness, on the other hand, you could argue is a support function, and there is a lot more to preparedness than preparing to respond. There are protection functions. As a matter of fact, you go through all the six critical functions outlined in the homeland security strategy. Many of them have a preparedness function to it, and so what we argued for in the report is splitting them, going back and basically having a FEMA which does the traditional things FEMA does, and then grouping preparedness really with all the outreach activities of the Department, State and local coordination, the domestic preparedness, the grants, the private sector coordination, critical infrastructure, transportation policy, and putting it under a single Secretary of Protection and Preparedness.

So above all, what you could get is somebody who is really looking coherently at the whole picture and really making decisions on where are we going to get the biggest bang for the buck? Where can we really get our best investment? How can we really make these things work together?

So those are the three principles that I would propose that should guide the next steps, and very quickly. I think there are two courses of action. We recommended in our report was to create a Presidential commission. I think that was kind of 9/11 Commission stars. But quite frankly that recommendation was made before both Houses made a decision to have a permanent committee to focus on the management of the Department. I think having that now provides a new opportunity to maybe do things differently, and what I might propose is a three-step process.

One is fix management first, create the Under Secretary for Policy, create an Under Secretary for Protection and Preparedness. Create strong COO functions in the Deputy Secretary, so we get rid of the dotted line thing which I think is simply not working. Abolishing the Under Secretary for Management. Abolishing the Under Secretary for Preparedness and Response. Cleaning up the management structure, making it very tight.

The second step is maybe we should steal a page from Goldwater-Nichols and establish a QSR, Quadrennial Security Review. And in the first Quadrennial Security Review, we should task the Department to review not just its resources and missions, but to do that in light of making assessment about envisioning the future, tell us where the Department is going to be 4 years from now, so we can make smart decisions about should we merge CBP and ICE and other things like that.

Now, in conjunction with that, I would also recommend that the Congress establish a national security review panel, much like we did the national defense panel when we did the first QDR, and it would have two missions. One mission would be to review the work of the QSR so we have an independent assessment about if their vision in the future is right, if their recommendations for organizational change are right, and also to look at how DHS fits in conjunction with all our other initiatives and all the other departments. And how it works in an interagency context and provide that report back to the Congress.

Then I think in 2006, the Department and the Congress could sit down and make some very far-reaching decisions about further organizational changes and perhaps other things that need to be changed. And with that, I look forward to your questions. Thank you.

Chairman COLLINS. Thank you. Mr. Wermuth

**TESTIMONY OF MICHAEL WERMUTH,¹ SENIOR POLICY
ANALYST, RAND CORPORATION**

Mr. WERMUTH. Madam Chairman, Mr. Ranking Member, distinguished Committee Members, thank you for the opportunity to be here and I am particularly pleased to be on this panel with so many distinguished colleagues and friends. Within the context of those four functional areas that you have asked us to address this morning, I am going to discuss six critical challenges facing DHS.

The first, as has already been mentioned several times, is this lack of robust strategic planning and analysis capabilities in the Department.

The second, and this is one of the items that goes to the very heart of what Senator Domenici was mentioning, is the lack of fully comprehensive performance metrics for the way we are spending homeland security dollars.

The third is the structure of the organization. We have already heard some of that. The fourth clearly is intelligence, particularly as it relates to the fulfillment of the DHS operational mission. And the last two, almost entirely external to DHS, have to do with some missed opportunities of both strategic guidance and oversight on the part of the White House and the Congress.

First, on border security. In our global economy, the United States is dependent on a variety of supply chains of both goods and services from all over the world. One that was not created with security at its core and we will hear more I am sure on that from Steve Flynn.

¹The prepared statement of Mr. Wermuth appears in the Appendix on page 79.

These supply chains involve government agencies, the global transportation and communications networks, the suppliers, marketers and users, but there is as yet no comprehensive approach to address all these various aspects of supply chains, not only in security terms but also the impacts that they have on economies, diplomacy, government stability, societal well-being, and much more.

RAND recently published a report entitled "Evaluating the Security of the Global Containerized Supply Chain,"¹ which reflects in its analysis of that issue the need for a more holistic approach to the entire spectrum of supply chain matters, and it is just one example of the way some of these issues need to be addressed in a more comprehensive fashion. And we respectfully request that this report be included in the record of hearing, Madam Chairman.

Chairman COLLINS. Without objection.

Mr. WERMUTH. We are in full agreement with James Carafano and others who have made recommendations for the Department to have a more robust capability to engage in long-range strategic thinking and only suggest that the entity that is created be called an Under Secretary for Policy and Planning to make it clear that its responsibilities include both of those important and somewhat different functions.

As we get better with security at the designated official ports of entry, for example, we would push terrorists and other criminal enterprises to unregulated points, and we must have a system in place to consider those second order effects and develop long-range plans and strategies that are flexible enough to meet the changing threats.

We have been asked to comment on recommendations for organizational change including the one that Jim Carafano just mentioned on the potential merger of CBP and ICE. We are not yet convinced that such a move is necessarily indicated and would be more flexible. Consider, if you will, that they do have fairly separate disparate functions. CBP performs ministerial tasks at the border points of entry. ICE performs critical law enforcement functions to identify actual or potential lawbreakers and engage in the arrest and seizure. That is not to say that those entities should not be in a central organization as BTS was originally envisioned and that they do not have a requirement in order to communicate with each other and to perform tasks that sometimes overlap.

But the skills required for the performance of those tasks may require different recruiting, retention, training, performance evaluations, operational procedures and the like and such a change without further comprehensive analysis of all the issues, structures and dynamics involved may not result in the intended consequences of more efficient and effective border security.

And in my written testimony, I have drawn some other analogies about the way other parts of our government are organized.

Second, in the area of transportation security, there must, and we argue can be, more holistic approaches that cut across old bureaucratic lines in various missions, and again to address Senator

¹ The report entitled "Evaluating the Security of the Global Containerized Supply Chain," appears in the Appendix on page 168.

Domenici's concern, we believe that one of those needs to be a move toward a more risk management approach to decisionmaking including better prioritization for resource allocations in the development of future strategies, plans and programs based on that risk management approach.

I mentioned TSA as an example in my written testimony and the rationale that would apply in that case. And there are many other examples about this strategic holistic approach to planning. Yesterday, RAND released a report that is in the news this morning on defending our commercial airline fleet against attacks using shoulder fired missiles, and there are some important conclusions in here about how to approach very difficult issues like that. We have sent electronic copies of that report to the Committee staff in preparation for today's hearing, and we would also ask that that report be included in the record of the hearing today.¹

Chairman COLLINS. Without objection.

Mr. WERMUTH. These better, more comprehensive, more authoritative measures of performance and effectiveness—a valid metrics program for the Department must be developed more completely than they have been and implemented, and that program will include clearly identified targets for specific performance at designated points in time or other proven techniques for evaluating the effectiveness of resource expenditures and other criteria.

For the structural side of transportation security, on the same rationale expressed above in connection with the proposed merger of CBP and ICE. It is still not clear without much further analysis that major changes should be made in other parts of the transportation and border security directorate.

Third, on emergency preparedness and response. Existing structures may not work and a thorough analysis is required in this area. DHS must have tighter geographic links to the field for closer coordination and more comprehensive collaborative arrangements with other Federal partners. And again, in the written testimony, drawing on both the issue of FEMA that Jim Carafano mentioned and the prevention piece of responsibilities as well as the preparedness piece, we have laid out some that we think should be considered in the deliberations of this Committee and others.

DHS should move quickly to implement its regional structure given the critical importance of closer cooperation with States and localities and the acknowledged differences in preparedness and response issues based on U.S. geographical diversity.

In the written testimony, I have offered other examples for external coordination including enhanced relationships with other Federal entities such as DOD and a long discussion about the better, more formal relationship that needs to be established between those two departments.

Fourth, for intelligence, clearly the Chairman and Ranking Minority Member have had an important role in the leadership of better intelligence across our entire government. I only hope that the vision that you have had for that new structure and process will prove to be effective in actual practice.

¹The report appears in the Appendix on page 168.

Clearly, DHS needs to have intelligence to help support its operational missions, but it is not yet completely clear what parts of intelligence DHS is expected to obtain for itself and what it receives from others.

In my written statement, I note important differences in strategic, operational and tactical intelligence, and some of the entities that have been established that will hopefully provide some more strategic approach to intelligence, but DHS clearly must have its own robust intelligence capabilities to perform fusion analysis and dissemination functions that will enable effective implementation of its own operational missions.

I also discuss in the written testimony the issue of closer coordination with entities at the State and local level who can help feed that entire intelligence process as well as issues related to security clearances and classifications, and I have offered some important discussion and recommendations that were contained in the fourth report to the President and Congress of the Gilmore Commission in December 2003 to support those suggestions.

Let me close on two points dealing with DHS oversight. It is a fact, of course, that DHS does not own everything related to homeland security. The Secretary has no authority to direct other Cabinet officials to do anything nor directly to command or control any assets other than those belonging to DHS.

The Executive Office of the President has important responsibilities to provide continuing strategic guidance and ensure proper coordination of all Federal resources through the development of national strategies and policies even beyond the Department of Homeland Security.

DHS should not be expected to develop the overall national strategy even though an important player. That is clearly a function for the White House. And Madam Chairman, respectfully, Congress is still part of the problem. It is still perplexing to me and I think to others that the Congress has not yet achieved a coherent logical process for handling these issues.

It does not seem to make sense to us that the Department of Homeland Security does not get its primary authorization in its entirety from a single committee in each House of the Congress. No other Cabinet agency is subjected to the same treatment. Madam Chairman and Members, thanks again for this opportunity. In our view, neither the Congress nor DHS should rush to any judgment about major changes in structure or authority without cautious, deliberate, well-informed circumspect debate and consideration.

Clearly, there are some changes that we and others have proposed that should rise to the top of the list for consideration. But please consider the fact that the Department of Homeland Security is relatively new, still just barely 2 years old, and men and women of goodwill both inside and outside of DHS are struggling to make the Department work more effectively.

DHS has already gone through much turmoil in its first 2 years of existence and it would be well to consider in that context the impact of yet more changes. I will, of course, be happy to answer any questions from the Committee and thank you again, Madam Chairman.

Chairman COLLINS. Thank you. Dr. Flynn.

TESTIMONY OF STEPHEN E. FLYNN, PH.D.,¹ JEANE J. KIRK-PATRICK SENIOR FELLOW IN NATIONAL SECURITY STUDIES, COUNCIL ON FOREIGN RELATIONS

Mr. FLYNN. Yes, good morning, Madam Chairman and distinguished Senators. It is an honor to be back here in front of your Committee testifying on this important issue and on this historic occasion of the first hearing of the Homeland Security and Governmental Affairs Committee. Like so many of us at this table and I know around the podium who were doing these issues before they were fashionable, it really says something about where we are to have you leading this Committee and to have such a distinguished group of Senators participating in it.

I would like to have my written testimony submitted for the record, but I would like to spend a few moments highlighting, I think, the rationale of how to keep ourselves focused on this, and then two or three items that I have that I think need to reinforce the messages that have been presented here.

In assessing where we are after 2 years, I think we really have to keep in mind what the challenge really is and where we started from. And there is no question, it is so important that we get this right because I maintain the position that what we saw on September 11 quite simply is how warfare will be conducted against the United States in the 21st Century.

The use of catastrophic terrorism directed at the non-military elements of our power, our civil society, and the critical infrastructure that underpins that power is how our enemies will confront us in the 21st Century. And when we, therefore, think about the allocation of resources for the defense of this Nation, we have to think about homeland security in tandem with the tremendous investment and sacrifice we have been willing to make in the national security arena.

In this context, we have a very daunting challenge if we talk about the asymmetric threat particularly dealing with something like a weapon of mass destruction coming into our society, and as we focus our attention and decide about the structure of this Department and how we resource it, and ultimately what emphasis and level of urgency we give this mission, I think we have to keep clear in our minds that we are dealing with a tenacious adversary. It has grown from probably an organization to a movement operating in about 60 nations around the world, who has shown that it has tremendous organizational capabilities to exploit the cracks in our globalized society.

Part of the thing that makes it such a daunting challenge is that, of course, homeland security just cannot be done at home. At the end of the day, the opportunities for exploitation and targeting is of global networks, of transportation and logistics, of energy, of finance, of information, that were driven in the globalization era of the last 20 years with four imperatives of the marketplace: How to make them as open as possible; how to make them as efficient as possible; how to make the network's use as low cost as possible; and as reliable as possible. And these were cascading. The lower the cost, the more users, the greater the reliability and efficiency,

¹The prepared statement of Mr. Flynn appears in the Appendix on page 98.

the more people were willing to depend upon them, but security was viewed as raising costs, undermining efficiency, undermining reliability, and putting pressure to close the networks.

We are dependent on our power, on global networks, that essentially have virtually no security built in. The job of this Committee overseeing the job of homeland security is, one, getting the nodes in the United States right, but also dealing with this in a globalized context that clearly expands beyond the jurisdiction of this one Department.

The second issue—so we have a daunting challenge that we have to sort of really keep our eye on when we look about what structure and the resource we put here. The other issue is that we have to really recognize how poor the starting line was we started from. The agencies that we have pulled together into this Department a little over 2 years ago were not in the strong state really for a decade or more. They did not get a lot of care and feeding from their parent departments at the time. That was one of the rationales for consolidating. They routinely did not get much in the way of appropriations either from OMB and so forth.

They started off hobbling to do their non-security mission, and now all of a sudden we have asked them to play this enormously important role of securing our Nation on the backs of basically broken agencies. So we start from a very weak baseline, and Coast Guard is a perfect illustration of operating an ancient fleet of ships and aircraft which we knew a long time ago we should be investing in. Now, their operations tempo is expanding enormously, and yet we have a 2 to 4 year plan to try to replace this capital plan. It simply will not be around in 3 to 4 years in most instances because we have run it into the ground. We are asking too much of it in the context of what this new mission requires and the traditional missions it must do.

All these other agencies have similar sort of legacy problems. And I ask us to keep in mind when we use the Goldwater-Nichols Act as an example, as it really is, of bringing things together, that was after 5 years of growth in the Department of Defense, when essentially those independent armed services were made whole after years of neglect after the Vietnam War made the opportunity for coming together something they could take on.

I do not think it would have worked so well in 1979 or 1980. It probably would have been a food fight then if they were all struggling just to do their core mission to try to get them to come together.

The final issue is that we are obviously dealing with merger and acquisition problems which any sort of 101 consultant will tell you that when you have for the first 18 months to 2 years of a merger even of just two companies, you are going to find rising costs, reductions in efficiency and losing good people. The public sector obviously makes that even more complicated. So we have to be willing to give a grace period obviously as we struggle to work through these because these are just practical challenges that we know from all elements of efforts to organize and manage.

But as we look ahead at the Department, while there are things that are sort of inevitable, this huge mission they are charged with, the low baseline they start from, the challenges of merging 22

agencies together, I would like to highlight, I think, particular problems that I think we can attend to relatively quickly and need to.

One is just simply the staff; there is no cadre of senior executives essentially being developed for this development. There is just one Senior Executive Service employee in this Secretariat for the Department of Homeland Security. If we had a presidential transition this time around, we would have had a mass exodus of those political appointees and the remaining players are detailees, people from the agencies who are essentially operating and trying to manage this environment. Now these are very dedicated people but all of us know we are a little bit of a bureaucracy. You tend to be more loyal to where you came from and where you are going back to than where you are at when it is in the context of a short-term assignment. We need to build a cadre of people who are basically providing some of the core base of capability.

The second—and this is just nuts—we do not have enough staff support for these senior managers. The Department, the Deputy Secretary of the Department of Homeland Security, the third biggest Federal Department, has a staff of five people to support his mission. The Chief Operating Officer of the third biggest Department undertaking the most daunting merger and acquisition has five people, and some of the lousiest office space in Washington.

We obviously need to give these players the tools to do the job right. There is no wonder why they are stuck in the in-box. Staff support is important and trying to professionalize this.

Next on the list is an issue I would argue of training these folks. This is an enormous new task we are asking people to do, and we are doing it with no training backbone in their system. Senator Warner certainly knows the Navy particularly puts a lot of investment in a naval officer. We do it because the stakes are enormous and because it is a very technically demanding environment. You do not want a guy in a ballistic missile submarine getting it wrong.

Forty percent of a naval officer's career is in training or education. Compare that to the Customs and Border Protection, training billets, zero, no time to do any training except during operations at a time when we are asking them to step up those operations.

We are asking people to do an increasingly complicated job. The Commissioner of Customs and Border Protection has this daunting job of one face at the border. All of us are relieved to not have to run through the gauntlet coming into our airports or coming across the borders, a very sensitive move, but you are asking a front-line agent, usually a very low pay grade, to be an expert on customs law, an expert on animal and plant health, to be an expert on immigration law, where your adversary is tenacious. It is trying to play around the gaps of that, and you do it with on-the-job training by a senior inspector who has also got a very full in-box.

We really need to look at how we resource the training of these people that we are depending upon to be our front line in this new war on terror.

Next, I would highlight the international dimension. I spent quite a bit of time overseas in various places. We do not have a lot of coherence. There are a lot of issues that are roused by various

activities of government. There are just not enough people in the Department to respond to these queries and to be able to handle real policy issues that are rising, nor are the State Department, USTR, those assigning people to the Department to do liaison.

And so what we end up with are crises that end up in the inbox and absorb a lot of senior management time to sort out when they could have been managed in advance without conflict.

The last thing I would raise is the fuzzy line issue, particularly with Department of Defense, over this issue of homeland defense and homeland security. The definition operationally does not work so well. The bad guys are not going to advertise they are coming from outside the United States to attack the United States. It is likely we will have an event here and then we are worried about follow-on attacks. If we have not merged more aggressively the homeland security activities and the Department of Defense activities, instead of having DOD essentially operating independently, we are worried about coming from the outside and DHS working from the inside. I just do not think operationally the threat is going to play out that way.

We need an ongoing, a very hard look at how we make that together. I know I am out of time, and with many of these issues we go on for a long time. I am honored that I have the chance to appear before this first hearing on this important topic and look forward to questions. Thank you, Madam Chairman.

Chairman COLLINS. Thank you. Dr. Falkenrath.

**TESTIMONY OF RICHARD A. FALKENRATH,¹ VISITING FELLOW,
FOREIGN POLICY STUDIES, THE BROOKINGS INSTITUTION**

Mr. FALKENRATH. Madam Chairman and Members of the Committee, I am very grateful for the invitation to be here this morning. I am particularly honored since this Committee has been the cradle of two of the most important pieces of legislation since the end of the Cold War, the Homeland Security Act and then the Intelligence Act of last year.

I will be very brief so we have a little time for questions before you have to go vote. My direct experience with the management of the Department ended in May of last year, when I left the White House and so I am really most knowledgeable about that period. But I will address some of the criticisms about the internal management of the Department. I am a little surprised by some of them, and I think some perspective is worthwhile here.

This is probably the hardest management task that any Cabinet member has ever been asked to take on. Not only are we in a war, not only are we asking these agencies to do more than they have ever done before, but we are asking them to conduct the largest re-organization in 50 years. And so, yes, there are some troubles with the management of this organization, but I will say, as someone who was involved in the initial design of the Department, that the performance of the Department's leaders has exceeded my expectations. I will agree with what Senator Lieberman said in the beginning, that no one thought this was going to be easy at the beginning and we were all right. This is very difficult.

¹The prepared statement of Mr. Falkenrath appears in the Appendix on page 103.

But I think that Secretary Ridge and Deputy Secretary Loy have done a very fine job, and I am grateful, Senator Akaka, for your kind words about Secretary Ridge. I think they really deserve more commendation than criticism for what they have done. There are some difficulties, of course. Another bit of perspective, however, is to identify one Federal Department or agency that has not had difficulties. They all do in various ways and it is sort of inherent in public sector management. Frankly, the studies that have been done, and my own experience with the Department, I am not persuaded that the management of DHS is substantially worse than any other department or agency in the Federal Government.

None of the other departments and agencies, by the way, have to deal with the reorganizational challenge that DHS has had to deal with. So that was my impression at least watching things from the White House. The Department does have a strategic plan. There is a public document that has been released by the Secretary that all of you, I am sure, have seen and your staffs have seen. And there is an internal set of milestones and goals, over 900 milestones and goals, all of which have a timetable and all of which have presidential appointees associated with every single goal who meet on a regular basis with the Deputy Secretary to go over how the Department is doing.

These goals were developed in consultation with the Office of Management of Budget and the Homeland Security Council, and so I think they are a pretty good strategic plan. I am not going to say everything is perfect in the Department. There are lots of difficulties, but these are extremely difficult choices and challenges that we have asked these appointees to take on, and I think on the whole they have done a pretty fine job.

With respect to Congress, I really think we should commend what the Appropriations Committee has done. They did exactly the right thing by reorganizing the subcommittees in the Appropriations Committee. Those two subcommittees have passed really fine bills on time, both years, with a minimum of earmarks and really following quite closely the President's request.

The Appropriations Subcommittees for DHS have become genuine partners in the Congress on how the Department has to perform because they know that this is now how it goes. There is going to be an appropriations bill done every year. It is taken extremely seriously. The Department needs to be highly responsive to their requests for information and consultation. The same could not be said for the authorizing committees. I am not going to belabor the point.

The 9/11 Commission made it, but it is really unfair circumstance to put the Department in on the authorizing side. The authorizing committee should do what the Appropriations Committee did in my judgment.

The third point: Reorganization. Heritage and CSIS have released a report recommending major internal changes in how DHS is organized. I think there is nothing sacrosanct about how DHS is organized internally, and there may well be changes that need to occur, but I think it is exactly the wrong time for a statutorily driven internal reorganization of DHS for four main reasons.

First, we are about to get a new Secretary in place. Give him the opportunity to get familiar with his new agency and his job and let him form an opinion and work with him in terms of what he thinks needs to be done.

Second, I think we need to follow through on the organization that we have established for DHS, not redo it all from the beginning.

Third, reorganization imposes a near-term penalty on performance. We know this very well. We have imposed a lot on various different parts of our government since September 11. Let us not impose any more is my judgment.

And fourth, the Secretary has certain limited reorganization authorities already, so he can unilaterally do things that he needs to do based on the authorities that were conferred in the Homeland Security Act. If Congress really wants to help him in the near term, I would recommend that you increase his unilateral reorganization authority, his ability to manage his Department flexibly.

He could use some additional reprogramming authority. He could use a better working capital account. He could use greater flexibility about the names and the number of under secretaries, and he could use a stronger reorganization authority, Section 872 of the original Homeland Security Act, which we worked on a lot. There are things that, if conferred on him, would help him right now, today, do his job. He does not need another statutorily driven internal reorganization. Now I think management of the Department is an important issue, and the overseers need to watch it very carefully. The Inspector General does. The GAO does. But I do not think it is the most important issue. I do not think it is his highest priority. I think the highest priority is what he does with his power. The Secretary of Homeland Security is one of the most powerful officers in the entire country, vested with vast regulatory authority and budgetary authority to do things out in the country.

And he has done a lot, I think. I am not going to give the laundry list of accomplishments, but there are a few things still that need to be done—which I have reflected on, and I wish I had managed to get more of them done when I was in government—but which I think are the highest priorities.

I will just tick them off. First, credentials and identification standard. This is a glaring gap, a systemic gap in our overall security system. The intel bill has a good provision about Federal standards for driver's licenses, but it does not go far enough. What we need is a national voluntary standard for secure identification that would become mandatory for all federally-controlled portals.

These issues I discuss in a little bit greater length in my written statement.

Second, we need to dramatically expand the amount of watch list screening that we do. We have two kinds of watch lists, name-based watch lists, which is lists of names and date of birth and that sort of thing, and biometric watch list. The name-based watch list is now consolidated at the terror screening center so that was a problem pre-September 11, now fixed.

Biometric watch lists are still divided. Eventually they need to be consolidated. We spend billions of dollars trying to get terrorist identifying information. We need to use it. We need to use it at

every possible opportunity. This expansion of screening against watch lists needs to be inside the United States primarily the Secretary of Homeland Security's job, and I urge you to encourage him to do that and to enable him to do it. Abroad, many officers are involved in it. He needs to assist.

Third, the defining characteristic of the September 11 attack was that al-Qaeda attacked a system in our midst that was inherently dangerous that we had become complacent about—airplanes—and was able to have catastrophic secondary effects on that attack. We have now taken care of that. Airplanes are no longer in that category.

Fortunately, there are a finite number of other such targets that are in that category. One, in my judgment stands out above the rest as uniquely dangerous and acutely vulnerable, and that is hazardous chemicals, in particular toxic-by-inhalation chemicals, ammonium, methyl bromine, phosgene, and chlorine.

These are basically World War I era chemical weapons which we move through our cities in extraordinary large quantities and quite low security. I am sorry to say since September 11, we have essentially done nothing in this area and made no material reduction in the inherent vulnerability of our chemical sector. If a terrorist were to attack that sector, there is the potential for casualties on the scale or in excess of September 11. I hope it does not happen, but it is just a fact that this is the case.

This needs to be the next big push in critical infrastructure protection. The Executive Branch has the authority to regulate this area when it is in transport, when it is being transported. It needs no new statutory authority there. It just needs executive action.

We do need new statutory authority if we are going to take care of the facilities because we cannot currently regulate the facilities, but we can if it is in transport. It is my biggest single concern for critical infrastructure protection. It is the one target which I think fits exactly into what Senator Domenici said, priorities. This should be the highest priority. The other ones do not matter nearly as much. This one does.

Fourth, we have made great progress on securing our air transportation system, substantial progress securing our maritime transportation system, very little on ground transportation systems, very little on rails, mass transit systems, trains and trucks. There is no silver bullet. There is nothing we can do, but we need a coherent program to deal with these vulnerabilities. It will involve some combination of access control sensors, telematic tracking, and geo-fences. There are things to be done. We need a push there. DHS needs to lead it.

Finally, and I apologize, terrorism insurance. The Terrorism Insurance Act will expire this year. Primary insurers have dropped terrorism insurance from their general commercial policies and so now there is basically no buildings in all of America that are insured against terrorism risk. We should reauthorize the Terrorism Insurance Act and mandate that all general commercial insurance policies include terrorism risk coverage.

Thank you very much for your attention and I am happy to take any questions.

Chairman COLLINS. Thank you for your testimony and thank you all for excellent statements. Dr. Flynn, you made a very good point in your comments about the legacy problems that some agencies brought to the new Department. The Coast Guard despite the strong support of many of us here had been underfunded for years. The INS was possibly one of the worst managed agencies in the Federal Government. And those problems did not disappear when the new Department was created.

The Department has, however, now been in existence for almost 2 years. Looking at the record of the Department and evaluating its success and integrating the various components and pursuing policies to make us safer, what overall grade would you give the Department if you had to assign a grade to it?

Mr. FLYNN. I was always a hard marker. My students complained about it. Again, one thing I highlight in my written testimony here, the people who are in Nebraska Avenue working these problems are the most selfless hardworking people in this town. But I think because of the reasons of what I lay out here I think we are in a C minus kind of state right now, and again it would be almost impossible not to be given the challenges that are confronting them, but this is a war on terror.

We are treating the overseas dimension of this with a tremendous level of urgency and with a real commitment of resources and we are treating this a bit like we are going through Social Security reform stuff. It is like an ongoing process, better government kind of thing, and I do not think we are adapting to the nature of warfare moving in this direction.

It clearly has worked, when we first deliberated this in the Hart-Rudman Commission about the need for consolidation, it was really because the parent agencies were not very good advocates for particularly the security mission, but often most of the other missions of these particular departments, whether it was Customs at Treasury or INS at Justice or Coast Guard at DOT, particularly. I think the Secretary has been an enormously strong advocate for his organization, but he clashes with other competing budget priorities and his issues are not looked at in the same budget column, of course, of our national security investments are made.

His are looked at vis-a-vis other domestic priorities, and if we are saying that the nature of warfare has changed and that line has blurred, then I think we really need to look hard. Is another weapon system vis-a-vis what needs to be recapitalization of the Coast Guard? How do we have that conversation right now because clearly there is security value to both, but how do we carry on the conversations of inevitable tradeoffs of the setting of priorities?

Chairman COLLINS. Dr. Falkenrath, you have a different vantage point. What overall grade would you give the Department for its first 2 years?

Mr. FALKENRATH. Well, I, too, was a very hard grader when I was on the faculty and I would give it an incomplete. I do not think I would give it a grade. It depends what the curve is. And here, whose curve do you want to use? There is a lot more to be done. No question about it, but a lot has been done as well.

And if you want to look at the glass half full or half empty is sort of perspective. I think half empty tells us all the things that still need to be done.

Chairman COLLINS. Let me ask you this then. If you look over the Department's record, what would you say has been its greatest accomplishment during the past 2 years and what do you think has been its most disappointing failure?

Mr. FALKENRATH. The greatest accomplishment, I think, is to create a presence and an entity to which we can give missions that previously did not have homes. So we now have a place to go and say we need a domestic protection plan for America as we go to war with Iraq. Before we did not have anywhere to do that. We now have a Cabinet Secretary who wakes up every morning with vast authority who has security in his job title and knows his job is to advance this cause whenever he had the opportunity.

Previously to September 11, we did not have that. We, at the White House, could go to a place and say we need to develop a plan to deal with problem X, which previously did not fit into any coherent boundaries, and so that now exists and I think it is a major accomplishment that they became responsive to those sort of unconventional requests.

The major disappointment—there are a number of them that I have. I think it is the third thing that I mentioned, which is the chemical security system. We took a lot of action to secure air transportation systems, we have done a bit on ports, and containers. I think this one stands out as an enormous vulnerability that we had the authority to address. It exists already, at least for transportation, and we failed to do so. I certainly take some responsibility for that.

Chairman COLLINS. Dr. Carafano, same question for you. Greatest accomplishment of the Department in the last 2 years and most disappointing failure?

Mr. CARAFANO. I think the grading question is actually the greatest question, and the reason for that is because you can not give the Department a grade because there are lots of things going on in the Department, some of them going extremely well, and some of them going extremely poorly, so if you give a grade of C minus, that is an average of 15 different things, and that is exactly the point. The Department is not moving forward as a coherent entity. It is moving forward as a bunch of individual programs.

Basically what we have done is create four demi-departments who are moving along at various different stages depending upon how they are run and how they are organized and how they are funded. The biggest problem is the inability to answer the question of where do I get the biggest bang for the buck? If I have 5 bucks to invest tomorrow, where I can invest it and get the most security? The Department cannot answer that question. The great success, of course, is that we have created the Department. It is a place full of absolutely wonderful men and women who work very hard every day to make us safe, and I love them all dearly, and they are doing a terrific job.

But they need to be able to do their job more efficiently and effectively and they need as a coherent body to be able to answer the question. If we have \$10 to invest tomorrow, explain to me how I

can make this investment and get the most for the \$10 I am investing, and they simply cannot do that right now.

Chairman COLLINS. Senator Lieberman.

Senator LIEBERMAN. Thanks, Madam Chairman. I apologize to the witnesses whose testimony I missed. I had to go to the floor, but I have read most of them and will read the rest. Chairman Collins asked you to grade the Department. I want to in some sense ask you what you think the plans for the next semester should be, which is to say that Judge Chertoff is going to be coming before the Committee soon, nominee for Secretary of the Department of Homeland Security.

I want to ask each of you, if you were coming before us as the nominee, knowing all that you know about the Department, what would be your top two priorities that you would state to us? Mr. Skinner.

Mr. SKINNER. The new Secretary certainly is going to have many challenges. I think the most important thing that he is going to have to address, though, is reaching a consensus among all the elements within the Department, each with their own set of priorities and each competing for the limited resources that are provided the Department of Homeland Security, on exactly what are the department-wide priorities, what do we want to accomplish this year, what we want to accomplish in 5 years, with the resources that we know that we have available.

Now this is going to require development of a strategic plan. I know the Department has a strategic plan, but I am talking about an operational plan that is developed at the highest level, possibly under an Under Secretary of Planning and Policy as the Heritage Foundation has suggested, but somewhere at that level, a plan that clearly sets forth what the priorities are, a plan that clearly articulates what our goals are.

Senator LIEBERMAN. Right.

Mr. SKINNER. A plan that specifies the costs associated with the goals, with milestones, that is time frames when should we attain those goals, with performance measures and related evaluation tools, so that we can gauge progress and so that we can assign accountability.

Senator LIEBERMAN. I appreciate the answer. In some sense it is a response to what Senator Domenici asked earlier which is we cannot do it all, but—

Mr. SKINNER. Yes.

Senator LIEBERMAN. And we know that. We cannot cover every risk, but we need the Department to help us with a plan that sets priorities, and the plan that they have now which was adopted in I believe 2002 is very vague and lacks any specifics. Dr. Carafano, what would your top two priorities be?

Mr. CARAFANO. Well, first, I would create a management structure that would allow the Secretary to impose his will on the Department much in the way the Secretary of Defense can impose his will on the Department of Defense to make it do what he wants.

The second thing I would do is create that strategic vision of where do you want the Department to be in 5 years, and what do you want it to be doing, and then I would use that vision to drive my resourcing and organizational decisions.

Senator LIEBERMAN. So statutorily now, you think the Secretary of Homeland Security is weaker than he ought to be?

Mr. CARAFANO. Absolutely in terms of his ability to create and disassemble under secretaries. I think he needs authority to do that because I think there is some movement there. I think in the Chief Operating Officer realm, I think there is sufficient legislative authority now for him to coalesce more power under the Chief Operating Officer and to create more authority under the deputy, and I would urge him to do that and not wait for legislative, although you could see where creating a Chief Operating Officer legislative authority in the Department that would permanently be there, I do not think would necessarily be a bad thing.

Senator LIEBERMAN. Thank you. Mr. Wermuth.

Mr. WERMUTH. You were not here for Richard Falkenrath's statement but it picks up on the point that Jim Carafano was just making. Clearly, the Secretary, if the Secretary were here asking this Committee what it could do to help, this capability and authority to do some reorganizational structure, whether it is the Under Secretary for Policy and Planning that some of us have recommended or some of these other things that Jim was talking about.

That is the first one. More authority to do things on his own as he sees priorities unfolding and then not to sound like a broken record, but on another point that I strongly agree with Richard Falkenrath about and I mentioned in my statement, that Congress provide a single source oversight and authorization authority for the Secretary to come to, and I know this Committee is making great strides in that direction, but even this Committee does not yet have authority over all of the programs and processes of the Department of Homeland Security.

Senator LIEBERMAN. Thank you. I think maybe CSIS and Heritage did a chart of the various committees involved in homeland security and it compares with the legendary Arlen Specter chart on health care in America and we ought to blow it up at some point for interest. Dr. Flynn.

Mr. FLYNN. Senator, I think there are two things that I would put on top of his list. One is to deal with the issue of complacency. I mean it really is the focal point in the U.S. Government to remind the American people about the ongoing threat that confronts us and the need for us all to work together as a collective society and work towards that, and that sort of public function I think he has to really make sure he continues to play the role that Secretary Ridge, I think, provided a very fine example of how you try to do that.

The second one is, I think, he simply has to come in and ask his organization and push across the U.S. Government, let us assume there is a bump in the night. A lot of the thinking that permeates the Department is if we have an event, we have failed. I think we have to act more grown-up than this. Our intelligence services are just not up to speed to give us a level of tactical information that is going to give us the threat-based with managed approach we are taking today. It will probably be a decade or so. Thanks to your law, we will get there probably in a decade.

This is a long time coming. You do not throw a switch and get the human intelligence to probe these networks and so forth. So we

will not have the advanced warning likely to prevent these. So I think the thing that can help drive change is you say what if this goes off, what is your plan, and force the players to see. That is what brings them together.

And just a quick example of that: We have a plan to close all our seaports and our borders should we have an incident involving a dirty bomb or something worse in our society. But the Federal Government today still does not have a plan how to turn them back on. They have not sat down and played it out how to do that. Well, trying to do that in a crisis, that can be done. That is not a cost issue. That is a planning and focus issue, but as soon as you begin that process of saying how do we turn it back on, you get people—the light bulbs go on, why we have to communicate, why we have to set the priorities, and the rest of it. So forcing the folks to really confront the reality of this threat and play back from it is something that I think could be very constructive.

Senator LIEBERMAN. Thank you very much. I am over time, but Dr. Falkenrath, would you give me a brief response?

Mr. FALKENRATH. Sure. Most of the important things that need to be done are outside of his direct unilateral ability to make happen, so people—all the under secretaries and the assistant secretaries—need to be appointed. He does not select them. The President does, and they are confirmed by the Senate.

Budget. It is decided by OMB, passed by the appropriators. Relationship with other Cabinet agencies, subject to the will of the other Cabinet agencies. Relationships with authorizing committees subject to the structure of the—within his domain, two most important things: Chemical security, as I talked about, and expansion of terrorist watch list screening.

Senator LIEBERMAN. Thank you. Thank you all. It has been extremely helpful.

Chairman COLLINS. Thank you. Senator Stevens.

OPENING STATEMENT OF SENATOR STEVENS

Senator STEVENS. Well, I am glad I came to listen to this panel. I am not sure but what you ought to listen to yourselves. Having been through 7½ years now of being Chairman of the Appropriations Committee and reviewing all the money that is spent by the United States on a discretionary basis, what I am hearing is more and more of the Federal Government ought to be in homeland security.

Homeland security affects every single agency in the government and you seem to be saying more staff in the Department of Homeland Security. We would much rather see them cooperate with the people who are out there now that know what they are doing. Should we put all the Department of Agriculture into Homeland Security because of the problem about importation of beef or importation of various substances?

Should we follow through in terms of this chemical problem which is a vast problem and travel, put more and more authority in the Department of Homeland Security or all interstate transportation or anything that is hazardous?

Now, guys, I think you ought to settle back. You should have been through World War II. The people of this country jumped in

and lot more people got involved from the grassroots and made the thing work very quickly. You seem to think everything has to come to Washington and be in Homeland Security in order to make this country secure.

I would urge that you go back and think a little bit more. You are all very brilliant men, but we have a government that is involved in AIDS, now \$15 billion in 5 years; in the tsunami, we are spending more than 50 percent of the money is being spent on that tsunami out there.

We have got more and more problems as far as terrorism in Indonesia, Philippines, etc. Money outside the Department of Defense and outside of Homeland Security is being spent over there in ways that you probably do not even know. I think Mr. Wermuth may. But as a practical matter, homeland security ought to be a concept that every single individual in the United States is part of.

And you are not going to do it by bringing it all to Washington and putting them in a new agency called Homeland Security. I hope that we can plan to diversify this agency and have it be the advisors to every entity in the government, whether it is the local police or the local fire department or the county sheriff or the FBI.

Now, this problem, each one of you has mentioned more money. Mr. Skinner, you did. I can tell you Homeland Security has had as much money as we could possibly afford in the period since September 11. More money than anyone ever thought they would get. And to have you tell us now that we have to have more money, I do not think is going to be there, and I urge you to help us find ways to do the money, use the money we have got to improve the system. And part of this jurisdiction is down in Commerce, by the way, and I understand what you are saying.

You seem to think that it ought to come here because we have jurisdiction of all transportation. Why should we have to—we will still have jurisdiction over transportation, but this Committee wants jurisdiction over transportation security. Can you split the line and tell me where it stops? Where is the problem about transportation and the problem of transportation security?

And the same thing exists throughout our system here. All the committees of this Congress have jurisdiction over entities that this Committee, that I am privileged to serve on, is involved with, too. I think you should help us find ways to coordinate the existing functions of government, where the money is already, and not say let us bring more of it out of those entities and put into Homeland Security to make sure we have enough money there.

I would be happy to visit with any of you along those lines privately personally, but I do not think there is going to be more money. Matter of fact, I know there is not going to be more money. [Laughter.]

So I would urge you to review your situation from the point of view how we can get the job done better with the money that is there now? Thank you very much.

Chairman COLLINS. Senator Warner.

Senator WARNER. Well, as my distinguished senior colleague is leaving, I think we have to find a midpoint for this pendulum. Mr. Flynn brought it home to me. I was once an under secretary of a

department of the government and had well over 100 on my staff alone.

I think we have to consider—first, I think Tom Ridge ought to get an A for effort. He has tried hard with what he has done and his team. But, folks, I think only by the grace of God have we been spared another attack here at home, and we cannot allow these expenditures to be directed in other areas without thinking, first and foremost, of our own security.

So I come somewhere between my dear friend and colleague of many years—a quarter of a century—here in the Senate, Senator Stevens, and I think we have to augment. But to a couple of a specific questions, we are likely to be faced in this Congress with a decision of a national ID card. Is this an agenda item the new Secretary ought to put on and begin to address? It is a divisive issue I want to think through very carefully. I frankly lean towards—I have not any reluctance—but I think the voices of those who do should be heard. But it is an important part of our security.

Do you have a view on that?

Mr. FALKENRATH. Yes, Senator, a national ID card is typically a mandatory card that the national government says every citizen must have and I do not think that is necessary here.

Senator WARNER. You do not think what?

Mr. FALKENRATH. I do not think that is necessary here. What is, I think, necessary and prudent, would be standards, a national standard for secure identification that would be voluntary and that any provider of identification documents could build to if they met the proper standards.

Senator WARNER. I think that is a very interesting idea. I would then turn to Mr. Flynn. You, I think, were right on target with your thoughts that we have to bring all of our assets to this Nation, but the military, active duty military and the homeland first responders to work together as a team. They are doing it now. It has got to be strengthened, but there is this famous old law, posse comitatus. I do not know whether you have ever studied the history, but it emanated from, I think, Grant trying to send some Federal people down to monitor an election in the South in the 1860's or something like that, and it has been very rigid. Does this need reexamination in the light of this allocation of responsibilities?

Mr. FLYNN. I think Michael Wermuth can probably speak most directly because of his experience at the Defense Department at the time when this was being worked on the drug war. I think there is enough wiggle room in it right now that it does not require us to make too much of an issue of it.

The real issue is the Department of Defense has basically said homeland defense is when the threat comes outside. Then they take the lead role and then preparing for that contingency. But everything we know about this adversary is that they are going to try to blend in. They are going to look like a passenger. They are going to look like an operator and so forth.

So the challenge here is really how does the Department of Defense get more engaged in the ongoing efforts with the Homeland Security to talk to the first responders, and do it in a real collaborative way, not that we have got a mission, DHS, you have got a mission.

Senator WARNER. Did you wish to make a comment, Mr. Werthmuth, on the posse comitatus?

Mr. WERMUTH. I would certainly agree that there is not a lot that needs to be done in terms of authority for the Department to be able to do significant things. We have got the Stafford Act, which not only authorizes the military to be used for natural disasters, but little known in the Stafford Act is also the capability to use the military in the event of an intentionally perpetrated attack. We have got the insurrection statutes. We have got two very specific statutes, one dealing with chemical and biological terrorism, another dealing with nuclear terrorism in Title 10, Section 382 in one case, in Title 18, Section 831 in another. So there is plenty of authority there.

We just need to do what I think you were suggesting, what Steve has also suggested. And articulate that more clearly so that we understand the roles and missions of the Department of Defense juxtaposed with the Department of Homeland Security so that everybody knows when and where those capabilities and authorities will be used.

Senator WARNER. Thank you. One of the principal inducements for me to join this Committee was, of course, first and foremost to work to get the maximum effect of both our forces abroad and the forces at home.

But I am privileged in my State to have one of the largest ports in America, Norfolk. And this issue of port security, where on the scale of resolving some of this, who is the expert on this? Because just start with this, what appears to be an insoluble problem, of what is the 8 million containers, what is the statistic a day that will land on our shores?

Mr. FLYNN. It is just about 20,000, about 9 million that came in last year, up to 30 tons of material per container. The basic challenge, Senator, is that I think we are really struggling to adapt to it. We have a process right now that if we target a container we want to look at, we now have the means to check it.

Believe it or not, on September 11 we could not do that. There wasn't gamma X-ray equipment in any of our seaports but one in Fort Lauderdale looking for stolen cars going out of the country. And we just did not have the manpower and resources. So we have made a big step forward with that.

The problem is that the intelligence that underpins our targeting is very frail because the quality of the manifests and so forth, and we are basically taking on 95 percent of the universe as low risk. I worry about for this adversary, if they spent 3 years acquiring a weapon of mass destruction, they will game out who we have defined as a low risk universe, and it turns out not to be rocket science.

They have things like Wal-Mart and Ford and GM written on them. And in that universe if something happens, the real risk is not that it will just get into the streets of Norfolk but the whole rest of the system would be contaminated. If it came from the 95 percent low risk, every mayor and governor would see every container as a high risk. In 2 weeks, we would shut down the global trade system.

So along with the chemical industry, that is a huge one for loss of life. Is our global manufacturing and retailing sector an incident away, potentially, from a real problem?

Senator WARNER. Thank you very much. I thank the Chairman. I just conclude by saying in the misfortune of another incident, this Committee will be held accountable for whether or not we did provide adequate funding for the various responsibilities. I want to give the support to the Chairman and the Ranking Member to achieve those dollars that are necessary.

Chairman COLLINS. Thank you. I would note that both the Chairman and the Ranking Member held a hearing on port security last year. We do expect to do more work in that area. I think it is our greatest vulnerability.

I would note that we have less than 5 minutes left in the vote. I would inform Senator Coburn that unlike the House we do not end votes on time. So I think there is time for you to question. I am going to go vote and I would ask you to put the hearing in recess after your questions, and I will get a full report on what you asked. And we will come back and allow any other Members who wish to come back to question and plus you will be shocked to know I have a few more for you as well. So thank you.

Senator COBURN. Thank you, Madam Chairman. I am sorry I missed some of your testimony. One of the things that strikes me—and if I missed this in your testimony, please bring it forward—but individuals talked about the Visa Waiver Program and substitute visas and port security and chemical risk.

But nobody is really focusing on our borders where millions of people come through illegally every year. You can do all you want on ports and you can do all you want on chemicals. But if you do not stop the transient crossing of the borders where we do not see them, where we do not stop them—or we have made the effort to make the difference, for we impact people who are coming across the border—why would you come through on a false visa when you can walk across either the northern or southern border almost without harm?

Do we have the technology to control our borders and what do we see happening on that to truly control our borders? Because we can do all these other things, every other interface. But I cannot imagine, my imagination of some chemical or some biological weapon coming into this country is not through one of our ports. It is coming across on somebody's shoulder walking across either the northern or southern border of this country, and anybody that would like to answer that, I would love to hear.

Mr. FLYNN. Well, Senator, I spent—before I got to September 11—I had a 2-year project where I essentially went along our borders, both in the Southwest border and the Canadian border and also visited our seaports asking front-line agents basically how you filter in the bad from the good given the volume and velocity.

And the short answer was we are not. At the ports of entry, we are just facing a tidal wave without the capacity. And the in between spots, particularly on the U.S.-Canadian border, we are talking a total of 300 Border Patrol agents that were then working there. That is about 1 every 5 miles. It is a challenge to think about in the broader context.

My basic conclusion was that you certainly need border capability, but it has to be just one of the layers and levers. What we really have, at least I think the opportunity in the North American context, is we have certainly a friendly neighbor to the north. The real threats are likely to emanate from outside the hemisphere. So it becomes important to think about the level of cooperation and intelligence sharing that you have with RCMP and other players on that side and development in Mexico.

We have got to put that in the context. The port of entry issue is about facilitating legitimate trade and travel. There is no issue on frontiers, the in between places, except for resources, if you want to police it. It is obviously a daunting challenge with 5,000 miles of real estate, a third of it water on the northeast, to think it would get adequately controlled. I started my career as a Coast Guard officer trying to patrol our coastline, and it is a huge task to imagine we have the means without tremendous resources.

Some tools are available, the UIVs and other kinds of stuff, but without the intelligence to decide where to look, there is a move afoot to say, well, let us monitor all the small vessels that are moving in our waters. Well, there are 6 million of them on the Great Lakes, 2 million Canadian, 4 million American. On a busy holiday weekend, there may be 2 million out there.

So monitoring with technology 2 million blips does not probably give you a whole lot of capability. You need the gum shoe, the guy who is out there seeing so many fish where there is no fish, and you need to have an intelligence apparatus.

So we certainly see at the border a real set of challenges, but most of those challenges emanate from beyond that border. We need a layer there. We need to push out and think and I think that is something that the Administration should be applauded on is the extent to which they recognize that we need a strategic depth and be able to work their way through that.

Senator COBURN. Dr. Carafano.

Mr. CARAFANO. If your goal is to reduce illegal entry and unlawful presence in the United States, you have to have a comprehensive solution that addresses internal enforcement, border security, and your relations with Latin America. And the point I will come back to, again from the report, is the Department of Homeland Security simply lacks the structure to create an efficient strategy to implement those three legs and effectively allocate resources against those three legs. And you have to do all three. Otherwise, it is really like trying to bail out the bottomless boat. I mean if you put resources into one without addressing the other two, then the problem simply will move other places.

Senator COBURN. OK. Anybody else? Well, the Committee will stand in recess until after the vote.

[Recess.]

Chairman COLLINS. The Committee will come back to order. Mr. Skinner, I want to ask your opinion of a very interesting recommendation that is in the CSIS and Heritage Foundation report concerning the potential merger or recommendation to merge the Customs and Border Protection agencies with ICE, Immigration and Customs Enforcement.

The testimony of Dr. Carafano makes the case that it would bring together under one roof all of the tools of affected border and immigration enforcement—inspectors, border patrol agents, special agents, detention and removal officers, and intelligence analysts, and realize the objective of creating a single border and immigration enforcement agency.

When I was in Los Angeles recently, I was very interested in the favorable reaction to this proposal among law enforcement officials from several different levels of government and different agencies including the FBI agent-in-charge, the sheriff of LA county, the director of the terrorist early warning center. All of them saw advantages from their perspectives in having this merger.

As someone who has studied the Department closely, what would your recommendation be? Do you think this is a good idea or not?

Mr. SKINNER. First, I would just like to point out we have not really studied the implications of such a recommendation so we cannot offer an informed opinion as to whether such a merger would be worthwhile or not.

I would caution, however, because we are in our infant stages, the Department is in its infant stages, and to reorganize again, in an area such as CBP and ICE, for example, may do more harm than good, but again that is just pure speculation on my part. It is something that I think should be studied very carefully as to what the impact would be on operations up and down the chain before a decision is made to do something to that effect.

Chairman COLLINS. Dr. Carafano, I discussed your resolution recently with a high level official at the Department because I am very intrigued by it and also because it did receive such a positive response from these law enforcement officials in California. He expressed to me the concern that it would have a very negative impact on employee morale if the two agencies were to be merged into one. What is your response to that?

Mr. CARAFANO. Well, I think that we are going to find all kinds of good reasons not to do something. I mean you really cannot counsel your fears. You have to have a vision of where you want to go. I really think that needs to be the driving force. I mean we need to decide how we want to do border and transportation security in this country and once we have reached that goal, then we need to structure to get there. This is very similar to the debate we had about should we split off and have a separate Air Force from the Army. It was based in large part on a vision of where warfare is going to be in the 21st Century, and the answer was, well, air power is going to be such a significant function, a domain, that it necessitates being its own separate identity.

And we live with the grace that people made that correct decision. I think we need to take the same intellectual energy to this. We need to take counsel of our fears and say where do we want to be in 5 years, and then let that drive our decision.

Chairman COLLINS. Mr. Wermuth, you mentioned that you thought that this should be studied more thoroughly. Is that something the RAND Corporation could undertake or how would you suggest that we determine whether this is a good idea?

Mr. WERMUTH. Well, without giving the Committee an advertisement for the work of the RAND Corporation, certainly we and oth-

ers have done this in different contexts for some of our defense clients as well as for other government agencies.

But without further study, I tried to highlight in my testimony the potential that with the different skill sets involved in inspectors at border ports of entry, and law enforcement people who actually go out and arrest folks, with those differences in skill sets, the recruiting and retention that backs that up, the training that applies differently to those different kinds of skill sets, without looking at that more closely, as I said, we are not yet convinced that the merger of those two is an essential requirement at this point.

And I used the analogy in the written testimony, in the military we have combat forces and we have combat support and combat service support forces. The skill sets are different. The training regimes are different. The recruiting and retention methods are different. The professional development to a very great extent in those two different kinds of functions is different.

We think that the same might apply. That is not to say this may not be the solution when you really dig into it and consider all those issues and balance the advantages or disadvantages of one particular structure or not. We just happen to think that it needs a great deal more attention and that is not to take anything away from the great work these guys did sitting around and based on their own great wealth of experience come up with some potential pathways ahead. We just think it needs more study.

Chairman COLLINS. Dr. Flynn, you have a lot of experience in this area. Do you think merging those two agencies would improve the operation of the Department?

Mr. FLYNN. It is a bit like, I think, where we were on September 11 when we first talked about merging. I cannot imagine how things would be any worse. I mean ICE is in a total disarray, and I do not know how it could be more demoralized than it is right now. It is an agency in search of a mission. But when I think functionally, and I go back to the Hart-Rudman rubbing which was about the course of national security in the 21st Century, the commissioners could have talked about how to reconfigure the national security establish to handle these threats.

What they recognized, though, was it was the non-military elements of these agencies that often gave them the particular skill set to deal with this kind of adversary. It was their regulatory role, their enforcement role, the relationships that gave them in these sectors that were critical, the Coast Guard is an illustration where you have both regulatory enforcement and military all in one organization, and you get a lot of value from that.

If you tried to break that up in the maritime arena, it would be very dysfunctional and very expensive to try to achieve it. I think we went in the wrong direction separating ICE from the Customs Service initially, primarily the immigration enforcement arm, because the intelligence, the incidence of criminality helps you set your framework for the risk analysis that is being done on your prevention and front-line players' expertise there.

And they, in turn—the enforcement folks—often need the leverage of the regulatory player to create the incentives. Wal-Mart plays by rules as other good companies do, not because of fear of criminal investigations. They happen very rarely and the fines are

not that big and so forth. The driver is the regulatory arm of that agency that says if you do not behave this way, we might have to slow things down, and so you really want that all, I think, under one roof versus separated from it. It is where it used to be. Of course, we are merging both Immigration and Customs but as we know with Immigration, we could not make things worse there.

But this decision to parse off I do not think was well considered. ICE is just not a functional entity today. That is what I hear from U.S. attorneys. It is what I see when I go out and talk to seaports and so forth. Nobody knows what their job is.

Chairman COLLINS. Dr. Falkenrath, what is your opinion of that recommendation?

Mr. FALKENRATH. I would not support it. First, I am not sure what problem it is trying to solve. There are serious problems in ICE. I agree with Steve. It is a troubled agency and has a lot of work still to do. There are some problems at CBP also. There are some problems within BTS also with the relationship with TSA. I am not sure what this reorganization solves.

Second, I think by doing it, you create new performance problems in the near term and you should give these agencies the opportunity to complete the reorganization they have been set to do and so forth. But the two most important reasons are, I think, the missions hang together pretty well as currently configured. CBP is our face to the traveling public and to the trade. And they enforce many different statutes and many different regulations at the border. And it is a law enforcement function, but it is one that deals with an enormous throughput every day.

ICE are investigators, mostly 1811s, mostly undercover. They can get Federal wiretaps. They are part of the JTFs. They are part of our drug task force that deal with things, and they run investigations against criminal behavior across borders, in the United States or in some cases abroad. Their core relationships are not with the traveling public or with the trade. It is with other Federal law enforcement agencies like the Secret Service or ATF or DEA or FBI.

So I actually think they hang together pretty well, and their missions are sufficiently distinct to justify the current configuration. Oddly, I think the bigger problem within BTS is between CBP and TSA, where there is a serious seam and a sort of dysfunctionality. Look at an international airport. You have on the top floor TSA screeners screening people going in. And on the bottom floor, you have CBP screeners screening people coming out. They both work for the Secretary of Homeland Security, but they have completely different backroom support structures.

That is where I would rather see integration, where we could save some money, get a little more flexibility. Both of them have targeting systems. TSA has the Office of National Risk Assessment. CBP has the National Targeting Center. They do basically the exact same thing. They have different contractors, different methods. ONRA has taken more out of the box approach and has gotten off the ground much more slowly. NTC is working right now today. They really should not be separate. They should be merged.

Chairman COLLINS. Dr. Carafano.

Mr. CARAFANO. I would just like to add one follow-up point.

Chairman COLLINS. That would be helpful.

Mr. CARAFANO. I do think we have to recognize that organization is really—and I am not saying that, again, merging this is necessarily absolutely the right answer, but all we have done is trade one set of problems for another. Before border inspectors and special agents worked together in one agency and that seemed very effective. The problem was that we split people from goods. Now, all we have done is created a new seam. Now, all the border inspectors work together, but all of a sudden somehow it is not appropriate for those people to work with investigators anymore.

So I do not know, I do not understand the advantage of what we have done, and I do agree with both Mike and Richard. I do think that this does require careful study, but I think the presumption that this is any better off than we have had before is certainly wrong, and I certainly agree with Stephen's point that these are agencies which are deeply troubled and I do not think we should just leave them alone and assume they are just going to get better.

Chairman COLLINS. Mr. Skinner, we clearly have differing views on the desirability of this merger, and I would like to ask you as the Acting IG to do a study of this issue and report back to the Committee, say, in 3 months or if that is too aggressive, maybe we would give you a little bit longer.

We do hope ultimately to do an authorization bill. For example, we have heard today about the desirability and there seemed to be unanimity on the need for an Under Secretary for Policy, and there are other changes that would require legal revisions, so it would be very helpful for us, and I would ask you to undertake that task to assist the Committee.

Mr. SKINNER. Madam Chairman, we will be happy to do that, and if I can I'll work with your staff so that we can set some time frames and milestones to report back to you.

Chairman COLLINS. That would be great. Thank you. Senator Lieberman.

Senator LIEBERMAN. Thanks, Madam Chairman. Thanks to you, Mr. Skinner, for your response to the Chairman's request which I appreciate and support. Dr. Flynn, I wanted to ask you a question about critical infrastructure, 85 percent of which is owned by the private sector. I know you have really focused on this and in your book you talk some about it.

There is a feeling, I think, among some people, maybe more than some, that the market forces that normally affect the private sector are essentially enough to get the private sector to do what it needs to do to protect itself and the country. I am talking about the critical infrastructure part of it.

I know that you feel, I believe you feel otherwise, and I wanted you to talk about that distinction a bit and evaluate where you think the Department of Homeland Security is now in its interactions with the private sector in regard to homeland security?

Mr. FLYNN. Thank you very much, Senator. This is an issue that I probably find myself focusing the most on of late, taking that our adversary, the one we need to worry about the most, is interested in economic disruption, not just loss of life. Our critical infrastructure has clearly become their target and 85 percent of them are privately owned, and we are talking about how we create the incen-

tives for that infrastructure to become more secure, again recognizing its baseline was it started off as open, low cost, efficient and reliable as those market drivers. Security was essentially pushed to the sidelines because there did not seem to be a threat that warranted making those investments.

So now we are having to integrate it in, and we should be doing it with some level of urgency. The Administration has stated in its homeland security strategy that there is sufficient market incentive for the private sector to protect itself. The data though after 3 years is that there has been very little investment by the private sector, particularly in an industry like the chemical industry but also in areas like food supply and so forth.

And I think the explanation for it is pretty straightforward. It is one I have talked with a number of CEOs about. And it is a tragedy of the commons problem. That is no single entity owns all of the critical infrastructure. And security is base line costs. If they therefore decide on their own to absorb those costs, protect their one element of it, it does not solve the problem because these folks will stake out the other players who are free-riders, exploit, but the whole infrastructure will be affected. There is also the practical issues. When it happens, Congress typically jumps in then, and the prescriptions may look different from the initial investments.

And I also think there is a liability concern. There is an issue that it is very difficult for the private sector to define how much security is enough, because it is the ultimate public good. And the fear is unlike other things like quality control and so forth, we say we agree as a trade association this is sufficient security, and we have an event, and the post-mortem is it failed. It was not enough.

Then there is some liability exposure. You acknowledged the threat but you did not do sufficient. Now the only way to vaccinate them from this is essentially when the public sector says that is a good judgment. We are willing to, knowing that this is a tradeoff issue, as we have been talking about all morning, we agree that that is an adequate level to achieve and we will hold the industry to it, so it is not a free-rider problem. The market playing field gets leveled.

The challenge here is that this is not going to happen by just illustrating best practices because you are not affecting that structure and that has been the focus of the Department's approach to try to garner the best experiences and then share that with the private sector.

The incentive structure is carrots and sticks typically. I think the issue is how do you form the standards? It has to be arrived at with their input because there are very few people in government who understand the sector sufficiently to make good calls about how much security is enough and what will work and not.

I advocate a very ambitious plan, something modeled on the Federal Reserve System which I am calling the Federal Security Reserve System. Just like in the financial sector, we had to find a way in which we had common rules, but we allowed it to largely keep it apolitical, and we want to make sure the expertise was resident to make good decisions. We found a framework that basically allowed that private folks agree how to clear checks and set up rules, the government to bound the risks that if something went

wrong, that we would not see the system failure historically with the panics that lead to the requirement for that Reserve System. We need to similarly adopt that, I think, kind of thinking into thinking about critical infrastructure.

The role for the Department then would be the public face that would interact with those I would argue regionally based to nationally based to make sure that government sanctioning of that is a good call, and the information that comes out of the Justice Department or that comes out of DHS informed it. But we have got to think about a structure and we have to think about incentives. And what we have is almost 3 years of data that shows that investments, real investments, making a big difference on protecting what is the basis for our way of life and is the most likely target is, in fact, getting the kind of investment that we need to make ourselves a more secure, more resilient society when we face this threat.

Senator LIEBERMAN. Very important and leaves a lot for us to think about doing in this authorization. Mr. Wermuth, I share your concern that the existence of the Department of Homeland Security does not alleviate the need for intergovernmental coordination because there is obviously a lot of other agencies of the Federal Government and beyond that have to be involved that are not part of the Department of Homeland Security.

There is, as you well know, the White House office dealing with homeland security. I wonder how you would assess the performance of that office, what it has or has not been able to do, and what if any recommendations you would make to the Committee about how to strengthen the office, if that is necessary, or to create some other entity to perform those intergovernmental outside of DHS functions?

Mr. WERMUTH. Thank you very much, Senator Lieberman, for the opportunity to address that, and I do some of that in greater detail in my testimony than I did in my oral remarks.

Senator LIEBERMAN. Right.

Mr. WERMUTH. And at the risk, of course, perhaps offending one of my colleagues at the table who was involved in that process, but I think Richard will agree, first, I mention things about just doing a better job of conceptualizing homeland security and explaining what that means. What is homeland security? Is it a subset of national security or is it something all out there by itself?

What is homeland defense as a component of that? Is that a subset of homeland security? Is that more a subset of national security? We have the principal architect, of course, of the 2002 National Strategy on Homeland Security sitting at this table, and we happen to think in evaluating that shortly after it came out that that was a very good start.

It is now 2½ years old and unfortunately it still only talks about combating terrorism, and we now know that certainly in the case of the Department of Homeland Security there is more to what DHS does, natural disasters and a whole lot of other things, than just combating terrorists.

So we have suggested, I suggested again in the testimony, that maybe it is now time to take a look at the national strategy for homeland security again and tie up some of these loose ends in-

cluding such simple things as terminology, which we happen to feel very strongly about.

In addition, suggested in the testimony and in other RAND publications that, perhaps understandably, the Homeland Security counsel staff and the White House has also been focused a little bit too much on current exigencies and not in that longer range strategic focus that we have talked about in terms of the Department itself. But in the case of the HSC staff and the White House, it clearly has a broader role.

Senator Stevens, of course, is right in several of the things that he says. The Department of Homeland Security cannot be responsible for everything. There are important pieces elsewhere in government that have responsibilities for some elements of homeland security, lower case, if you will, rather than Department of Homeland Security, upper case.

So there has got to be better strategic focus on the White House of bringing together all of those entities of the rest of the Federal Government and including some of our international considerations in the same way that we are suggesting that the Department itself needs to have a better strategic focus for its own operational elements.

I would argue that it is time that the HSC staff now perhaps move beyond being involved in perhaps more of the day-to-day operations of the Department and focus a little bit more on the strategic planning, the intergovernmental/interagency coordination functions that are called for here.

Senator LIEBERMAN. Thanks. Helpful answer. I am going to ask Dr. Carafano to comment on something that Dr. Flynn said and maybe he wants to respond, which is about the relationship between the Department of Homeland Security and the Department of Defense. His language was very good here. I thought he said the Pentagon has been keen to maintain its autonomy—we have seen that—by assigning itself the mission of homeland defense, which it defines as involving terrorist acts that emanate only from outside the United States.

And then he goes on and makes some points, and basically says that the artificial line drawn between homeland defense and homeland security needs to be—in some ways it picks up on what Mr. Wermuth has just said—needs to be reexamined with an eye toward expanding the operational support role the DOD will play in carrying out DHS's mission. What do you think about that

Mr. CARAFANO. I think Steve and I, exactly agree on that point. The creation of the term "homeland defense" was done by the Department of Defense so they could define what they want to do and what they did not want to do. It is an artificial line that has absolutely no utility as a doctrine or in terms of the deciding roles and missions.

And they should really be forced to get rid of it and we should have a term which is homeland security. So I think Steve and I exactly agree on that point. I think there are three areas where the Department of Defense needs to be a much better team player. Maritime security is clearly one. There should not be a gap between what the Coast Guard does and what the Department of De-

fense does. It should be seamless and it should be complementary. It is not.

Two is catastrophic terrorism. I mean no matter how much money we put in State and local governments, they are never going to have the capacity to deal with catastrophic terrorism, nor is it, and we are talking the tsunami style, tens of thousands of casualties, nor should they do that kind of investment. There is an appropriate, and Mike and I disagree on some of this, but there is an appropriate role here for the Department of Defense. They have always said that they will do that.

The last thing I want to see is the Department of Defense figure out how they are going to do catastrophic terrorism on the day after the catastrophic terrorist attack.

Senator LIEBERMAN. Right.

Mr. CARAFANO. We need structures and forces in place now that are designed to do this and do this well. I have argued in other places that if you built that kind of capability right in the National Guard that you would actually have a very useful force that could be useful for a range of homeland security missions and would also be very useful for post-conflict operations overseas and would also be used for theater support operations overseas.

So if you had it large enough and organized correctly, it would actually be a multi-purpose force which would have a wide range of utility and would prepare us well for the day that we all do not want to think about.

And then the third area really is in S&T. Quite frankly, there is just too much S&T going on in the Department of Defense which marries up very well, not in the specifics, but conceptually, and in terms of research and development and testing with what is being done, what needs to be done in homeland security. Weapons of mass destruction research, for example, is one classic example.

The fact that they are not welded at the hip in terms of gaining the efficiencies of what they are both doing is just wrong. So those are three areas that I think that much more could be done.

Senator LIEBERMAN. Excellent. You want to add anything, Dr. Flynn?

Mr. FLYNN. No, I completely agree, I guess. I think that captures it so well. And it has gotten so just where it is at in terms of dysfunctionality, shortly after the Department was created, Secretary Rumsfeld said that any request from the Department of Homeland Security for any asset of the Department of Defense would have to be cleared through his office. So this has made it very difficult. Unless Tom Ridge personally got on the phone and pleaded, you could not have any lateral kinds of connection, and it has been very structured under the Assistant Secretary of Defense, even where the Northern Command cannot talk to, they have to go through the Pentagon in order to deal with the Department of Homeland Security even though they play that critical role.

There is no question on the maritime that this is, and there is a distortion towards collecting of information and patrolling, but without thinking about incidence management or capitalizing on the kind of assets that we have with the homeland security agency. So it deserves a very good look.

Senator LIEBERMAN. Thank you all for the time you took to prepare your testimony and for your responses to our questions. Madam Chairman, this has been an excellent first hearing for the Committee and it really does say to us loud and clear that even though the oversight has not been as consolidated in this Committee or any Committee, as we would have liked, we kept saying during the floor debate put it somewhere else, but at least consolidate it somewhere.

We have a very important role here to play, whether the rules exactly say it as much as we would like or not, in leading the Congress in oversight, and further implementing the laws that are on the books now and improving them because we have come a long way, as you have all said since September 11 in raising our defenses. We have got a long way to go against a threat that is clear and present and potentially devastating. So thank you all very much.

Chairman COLLINS. Thank you, Senator. I am going to ask just a couple more quick questions, but you do not have to stay and hear them. Thank you. I would like to ask each of you if there is any agency or program that is now within the Department of Homeland Security that you think should be moved out of the Department and does not belong there?

Sort of the opposite question from what we have been discussing. Mr. Skinner.

Mr. SKINNER. Right at the moment nothing comes to mind. But I would like to give that some more thought. I never looked at it from that perspective. I have always been looking outside to see what should be coming in. I have never thought about that.

Chairman COLLINS. Thank you. Dr. Carafano.

Mr. CARAFANO. Yes, I would just like to add for the record that nowhere in our report to we advocate increasing the size of the Department, increasing the funding to the department or adding authorities to the Department. I do think one area which still requires some fine-tuning is in the area of bioterrorism response. I think the notion to try to split response of police between HHS and DHS has largely not been helpful. I am not really sure DHS needs a role in bio-shield at all. I am not sure that it needs much of a role—I know they have already moved the pharmaceutical stockpile back. But I just think that other than kind of a general supervisory role in terms of the overall response effort, I am not sure DHS needs to have much involvement in this area.

Thank you. And I appreciate your response to Senator Stevens' comments. I have a feeling I would hear that repeated across the panel.

Mr. Wermuth.

Mr. WERMUTH. As I was just getting ready to repeat them, Madam Chairman, because certainly our focus, the focus in this testimony and the focus in other contexts is not necessarily—in fact, I say very clearly the best measure of performance cannot be how much more money we are spending.

It has got to be a rationalization and a prioritization of resources. I have to agree nothing particular comes to mind that we would think should be moved outside the Department of Homeland Secu-

rity, but it certainly requires a close look to see whether that is the case.

Chairman COLLINS. Dr. Flynn.

Mr. FLYNN. I have to swim against the stream on the resource pitch. A lonely business here, but this is about national security. The President said we have a two-front war. And we are talking about a nickel on a dollar in terms of what we are spending on homeland security vis-a-vis what we are defending on national security. So if we are talking about resources, I think we have to look at the totality of the investment the American people are making.

They think national security is about protecting the Nation, and homeland security is clearly an element of that. So that is a big challenge that is out there. It is not that bigger is better. Most of what I have been advocating actually is much more push it out, but there needs to be a competent Department where we consolidate this.

In terms of pushing out, I do not see that and also I do not want this huge entity to take over, as Senator Stevens was sort of alluding that might happen ultimately, but it is recognizing that it is the non-security dimensions of these agencies that often give them the most value-added. It gives them the authorities. It gives them the relationships with the citizenry and the public sector. In a way that a Navy SEAL never can, a Coast Guard cutter can.

There is a much different sort of flavor to that interaction when that sort of thing happens, and it gives them the presence in terms of where they are in a space that we know the bad guys are going to pursue. So at the end of the day, we are really thinking about not saying rob Peter to pay Paul. If these agencies are—if Customs is incompetent in managing its trade rules, it will not spot a bad guy who is exploiting those trade rules to hide what he is up to, whether it is to launder or to potentially bring something in.

If the Coast Guard basically is not doing its job of fisheries patrols and so forth, it is not going to spot the terrorist who is pretending to be a fisherman but he is fishing where there are no fish. We are drawing on skills that we have to value and invest in, but we need to make sure we tether it into our national security framework because the threat requires it.

I think that is the kind of thinking we have to bring to the table versus stop doing this—public health—do not do public health, only bioterror. That is not a sustainable approach and it is a wrong-minded approach.

Chairman COLLINS. Dr. Falkenrath.

Mr. FALKENRATH. Senator, to your question, Plum Island. We should give it back to USDA.

Chairman COLLINS. Thank you. My final question I am actually just going to submit to you for the record, but just so you know what the issue is. We still have a coordination problem, and bioterrorism is a perfect example, between DHS and other departments, DHS and HHS in this case. We also have the problem with the two fingerprinting systems, one the FBI's, the other is DHS's, not being compatible.

I would like you to think and for the record respond to how do we deal with the problems, the coordination problems that involve other departments? Because I think those are at least as daunting

as the ones within the Department. When I think of how long it has taken to get a consolidated watch list and when you look at the investment in the Justice Department and DHS fingerprinting systems, and the fact that they are two different systems and the inefficiencies that produces, it seems to me we need to look at those issues as well, as well as what is going on within the Department.

So I will formulate a more precise question for the record for you on that.

But I do want to thank each of you for being here today and for sharing your expertise. I cannot imagine a more expert and interesting panel to start off the hearings of this new Congress. So I thank you very much for your contributions. The Committee has no more important mission than an oversight responsibility for homeland security, and that is why I wanted to begin the new year focusing on that issue.

I hope we can continue to call upon you for your expertise and I thank you for your participation today. The hearing record will remain open for 15 days, and this hearing is now adjourned.

[Whereupon, at 12:50 p.m., the Committee adjourned.]

A P P E N D I X

STATEMENT OF RICHARD L. SKINNER

ACTING INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

JANUARY 26, 2005



Good morning Madam Chairman and Members of the Committee:

I am Richard L. Skinner, Acting Inspector General for the Department of Homeland Security (DHS). Thank you for the opportunity to be here today to discuss the work of the Office of Inspector General (OIG) regarding major management challenges facing DHS.

During its first 2 years of existence, DHS worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the critical, core mission of protecting the country against another terrorist attack, has presented an inordinate number of challenges to the department's managers and employees. The Government Accountability Office (GAO) has noted that successful transformations of large organizations, under even less complicated situations, could take from 5 to 7 years. While DHS has made great strides toward improving homeland security, it still has much to do to establish a cohesive, efficient, and effective organization.

The OIG, based, in part, on assessments by legacy OIGs, Congress, the department, GAO, and others, has identified "major management challenges" facing the department, for inclusion in the department's Performance and Accountability Report issued on November 15, 2004. These challenges are a major factor in setting our priorities for audits and inspections of DHS programs and operations. As required by the Reports Consolidation Act of 2000, we will update our assessment of management challenges annually.

Our latest major management challenges report covers a broad range of issues, including both program and administrative challenges. A copy of that report is being provided for the record. In its response to the report, the department recognized the challenges and the potential impact the challenges could have on the effectiveness and efficiency of its programs and operations if not properly addressed. The department anticipates that the results of initiatives to address the challenges during FY 2005 should enable it to report significant progress next year.

The Committee has asked us to focus today on challenges related to border security, transportation security, integration, intelligence, and preparedness. I would like to highlight the significant issues that we have reported in these areas, which deal primarily with border and transportation security, and some of the work that we have underway or planned.

Before I discuss the details of our work, however, I believe it is important that we give credit to the thousands of dedicated, hard working DHS employees who are genuinely committed to securing our homeland and making the department a model for the entire federal government. No one here can deny that our nation is more secure today than it was prior to September 11, 2001.

I also wish to point out that the department has been very responsive to and implemented a number of the recommendations made by our office. We look forward to establishing a positive working relationship with the new Secretary, and continuing the momentum already underway toward building an effective, efficient, and economical homeland security operation—one that is free of fraud, waste, and abuse.

BORDER SECURITY

A primary mission of DHS is to reduce America's vulnerability to terrorism by protecting the borders of the U.S. and safeguarding its transportation infrastructure. Within DHS, these responsibilities fall primarily with the Border and Transportation Security (BTS) Directorate.

Two organizations within BTS are responsible for enforcing the nation's immigration and customs laws. Customs and Border Protection (CBP) inspects visitors and cargoes at the designated U.S. ports of entry (POE) and is responsible for securing the borders between the POE. CBP's primary mission is to prevent terrorists and terrorist weapons from entering the U.S., while also facilitating the flow of legitimate trade and travel. Immigration and Customs Enforcement (ICE) is the investigative arm of BTS that enforces immigration and customs laws within the U.S. While CBP's responsibilities focus on activities at POE and along the borders, ICE's responsibilities focus primarily on enforcement activities related to criminal and administrative violations of the immigration and customs laws of the U.S., regardless of where the violation occurs. CBP and ICE also have employees assigned outside the U.S. to enhance the security of our borders.

In December 2004, the Heritage Foundation recommended merging CBP and ICE and eliminating the Border and Transportation Security directorate. According to the Foundation, the merger would bring together all of the tools of effective border and immigration enforcement – Inspectors, Border Patrol Agents, Special Agents, Detection and Removal Officers, and Intelligence Analysts – and realize the objective of creating a single border and immigration enforcement agency. Eliminating BTS would remove a middle management layer allowing the combined CBP-ICE to report directly to the Secretary via the Deputy Secretary. Insofar as we have not studied the implications that such a reorganization would have on the department's border security initiatives, we are not in a position to address the pros and cons of such a reorganization.

The third organization within BTS that plays a major role for protecting the borders of the U.S. and safeguarding its transportation infrastructure is the Transportation Security Administration (TSA). TSA's primary security improvements have focused on aviation, with the hiring of over 60,000 passenger and baggage screeners, installing electronic passenger and baggage screening technology at the nation's airports, and greatly expanding the Federal Air Marshals Program, which is now organizationally located in ICE.

Other organizations within BTS have border security related responsibilities as well, such as the US-VISIT Program Office and the Federal Law Enforcement Training Center (FLETC). The US-VISIT Program Office is responsible for the development and fielding of the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, DHS' entry-exit system. It also coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS). FLETC, also a BTS component, provides career-long law enforcement training to 81 federal partner organizations and numerous state, local, and international law enforcement agencies.

Also, although not organizationally housed within BTS, the U.S. Citizenship and Immigration Services (USCIS) plays an important part in DHS border security. USCIS is responsible for reviewing and approving applications for immigration benefits. While not a law enforcement agency, USCIS ensures that only eligible aliens receive immigration benefits and identifies cases of immigration benefit fraud and other immigration violations that warrant investigation.

Needless to say, DHS faces several formidable challenges in securing the nation's borders. Our audit and inspection program has attempted to address some of the challenges. These include: developing effective overseas operations; preventing terrorist weapons from entering the U.S.; and tracking the entry and exit of foreign visitors.

International Operations

As the Heritage Foundation's report aptly pointed out, our nation's homeland security does not stop at America's geographic borders. DHS faces international challenges in protecting our borders. Provisions in the visa issuance process and other programs to promote international travel create potential security vulnerabilities that may allow terrorists, criminals, and other undesirables to enter the U.S. undetected.

For example, DHS must address security concerns identified in the Visa Waiver Program (VWP). The VWP enables citizens of 27 countries to travel to the U.S. for tourism or business for 90 days or less without obtaining a visa. These travelers are inspected at a U.S. POE, but have not undergone the more rigorous background investigations associated with visa applications. In an April 2004 Inspection, we reported our concerns regarding the exclusion from the US-VISIT program of travelers under the VWP. In September 2004, BTS began requiring travelers from VWP countries to enroll in the US-VISIT program, and renewed its efforts to conduct required country reviews.

However, DHS continues to experience problems in identifying and detecting aliens presenting lost and stolen passports from VWP countries at ports of entry. Shortcomings in procedural and supervisory oversight permitted some aliens presenting stolen Visa Waiver Program passports to enter the United States even after their stolen passports were reported, watch-listed, and detected. New information on lost and stolen passports provided by Visa Waiver Program governments was not routinely checked against U.S.

entry and exit information to determine whether the stolen passports have been used to enter the U.S. In addition, there was no formal protocol for providing information concerning the use of stolen passports to ICE for investigation and apprehension of the bearer.

In addition, lost and stolen passport problems are complicated by the lack of international standardization in passport numbering systems that can result in a failure to identify *mala fide* travelers using stolen Visa Waiver Program passports even when the theft has been reported and the information is available in DHS lookout systems. This occurs because stolen passports are reported using the passports' inventory control numbers (ICNs), which are entered into the lookout systems. However, inspectors routinely enter just the passports' issuance numbers into the lookout systems, and therefore do not match the reported stolen ICNs, resulting in undetected stolen passports. While we applaud BTS' efforts to promote a change in the International Commercial Aviation Organization (ICAO) standard to a one-number passport system, it will take years once the new standard is adopted for the two-number passports to be removed from service. Interim measures are needed to reduce this vulnerability. In response to our concerns regarding the use of stolen Visa Waiver Program passports to enter the United States, BTS has taken steps to conduct systematic reviews of admission records to check for previous uses of newly stolen passports.

Further, DHS also must address issues identified with its visa security program, which stations DHS officers at U.S. embassies and consular offices overseas to review visa applications and perform other law enforcement functions. Because of its limited resources, BTS used temporary duty officers who often did not have the required background or training, including language skills, to perform effectively as visa security officers. For example, nine of the ten temporary duty officers who have served or are serving in Saudi Arabia did not read or speak Arabic. This limits their effectiveness and reduces their contribution to the security of the visa process. In response to our report, BTS advised that it would: stop using temporary duty officers and begin using permanently assigned officers at its visa security offices; develop a staffing model to ensure only qualified officers serve in these positions; and develop a training program for visa security officers. While BTS agreed with us in principle regarding the need for language training, BTS officials said that, because of funding concerns, it would provide language training "as necessary and to the extent possible."

As a result, the full intelligence and law enforcement value that Visa Security Officers could add to the existing inter-agency country teams has not been achieved. In response to our report, DHS advised that it has developed a near-term plan for deploying visa security officers for FY 2005 and was planning for additional deployments.

With respect to international travelers, two major border security challenges confront the department: the divergency in the biometric systems used to identify travelers, and the substantial differences in the levels of scrutiny given to different classes of travelers.

Biometric Systems. We have all seen the glaring deficiencies of name-based lookout lists: for every known terrorist there are many innocent people with the same name. And for every name, there are variants and misspellings. Biometric identifiers are the only reliable and practical way to tell people apart.

The FBI uses ten rolled fingerprints in the IAFIS to document criminal activities. The former INS, now within DHS, used only two index finger prints to create retrievable records for travelers in its Automated Biometric Identification System (IDENT). As has been widely reported, the two systems have not yet been integrated, so some travelers are run through one system, and then sometimes the other, at ports of entry. The CBP agents are required to check both systems when possible illegal aliens are apprehended.

The international standards for passports are developed through ICAO. The United States is one of several countries whose citizens are not routinely fingerprinted for licenses or identification cards. In the past, the U.S. has lobbied ICAO to use facial recognition rather than fingerprints as the required primary biometric identifier in passports. Public accounts suggest that the experiments to date using facial recognition (at Logan Airport, among others) yielded meager results. At our borders, meanwhile, we increasingly rely upon fingerprint scans to tell people apart. The difficulties in achieving international consensus on this subject are daunting. More daunting and far more obvious, however, is the fact that the United States cannot afford to implement both biometric capabilities at each port of entry, it must settle on one. We – the United States Government – need to decide soon which biometric is the most reliable. Then we need to apply that standard to our own identity and travel documents, as well as for foreign travelers. We cannot do this in a vacuum, however; we need international cooperation to establish a global standard.

Levels of Scrutiny. The second challenge relates to the inconsistent levels of scrutiny to which travelers are subjected. Everyone knows that some nonimmigrants need visas, but many do not. Less well known is that some do not even require passports. Immigrants, some of whom spend little time in the U.S., receive medical examinations and background checks, but nonimmigrants, some of whom remain legally for many years, do not.

Usually, travelers from visa waiver countries do not require visas, but, depending on the claimed purpose of their trip, they sometimes do. Most citizens of Canada and Mexico do not need visas or passports to enter the United States, and we do not always record their names, or check them against our databases, though we do check their automobile license plates at land POEs. During FY 2002, 104 million visa exempt Mexicans constituted 24 percent, and 52 million visa-exempt Canadians constituted 12 percent, of all admissions.

U.S. citizens reenter the country with the least scrutiny of all, and frequently require no passport. Foreign travelers who can successfully pretend to be Americans get the same special treatment, of course, as documented by the GAO in its May 2003 report,

“Counterfeit Documents Used to Enter The United States From Certain Western Hemisphere Countries Not Detected” (03-713T).

The US-VISIT system screens only nonimmigrants with visas, or visitors using the provisions of the Visa Waiver Program. According to fiscal year 2002 statistics, the approximately 15 million VWP visitors accounted for 3 percent of U.S. admissions, while 19 million travelers with nonimmigrant visas accounted for 5 percent. In essence, US-VISIT screens fewer than 9 percent of the people entering the United States. At land borders, where travelers with visas or using the VWP are a rarity, the percentage of crossers screened by US-VISIT is also very small: less than 3 percent.

No one designing a border security system from the ground up would create such a hodge-podge of processes with so many potential security gaps. If we are to be serious about border security, we will need to rationalize our border crossing processes. People are not always who they claim to be, and terrorists and criminals will try to assume whichever false identity will get them the least scrutiny as they enter and depart our country.

Preventing Terrorist Weapons from Entering the U.S.

Since September 11, 2001, CBP's priority mission is detecting and preventing terrorists and terrorist weapons from entering the U.S. A major component of its priority mission is to ensure that oceangoing cargo containers arriving at the seaports of entry are not used to smuggle illegal and dangerous contraband. To test controls over importing weapons of mass destruction, ABC News was successful in two attempts at smuggling depleted uranium into the country. On September 11, 2002, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium was shipped from Europe to the U.S. undetected by CBP. On September 11, 2003, ABC News reported that the same cylinder was smuggled to the U.S. from Jakarta, Indonesia, again undetected.

In the first smuggling event, ABC News reported that a steel pipe containing a 15-pound cylinder of depleted uranium, which was shielded with lead, was placed in a suitcase and accompanied by ABC News reporters by rail from Austria to Turkey. In Istanbul, Turkey, the suitcase was placed inside an ornamental chest that was crated and nailed shut. The crate containing the suitcase was then placed alongside crates of huge vases and Turkish horse carts in a large metal shipping container, and then loaded onto a ship that left Istanbul. Based on data contained in the Automated Targeting System, the crate was targeted as high-risk for screening by the U.S. Customs Service (Customs). ABC News broadcast on September 11, 2002, that Customs failed to detect the depleted uranium carried from Europe to the U.S.

During the second smuggling event, ABC News placed the same cylinder of depleted uranium into a suitcase, and then placed the suitcase into a teak trunk. The trunk, along with other furniture, was loaded into a container in Jakarta, Indonesia, and then transshipped to the U.S. from Tanjung Pelepas, Malaysia. This shipment was also

targeted as high-risk for screening and subsequently inspected by CBP personnel, but was then allowed to proceed from the port by truck.

In a classified September 2004 report, we cited several weaknesses that occurred at the time of the two incidents that made the container inspection process ineffective. The protocols and procedures that CBP personnel followed at the time of the two smuggling incidents were not adequate to detect the depleted uranium. CBP has since enhanced its ability to screen targeted containers for radioactive emissions by deploying more sensitive technology at its seaports, revising protocols and procedures, and improving training of CBP personnel.

During FY 2005, we plan to conduct a follow-up audit on the issue of radiation detection. The audit will determine to what extent CBP has a complete and workable plan for deploying and effectively operating radiation portal monitors at major U.S. seaports, and how the new technologies that CBP is deploying will impact operations at the ports.

Tracking the Entry and Exit of Foreign Visitors

Keeping track of people entering and leaving the U.S. is necessary to prevent terrorism, narcotics smuggling, and illegal alien smuggling, and to enforce trade laws and collect revenue, all while facilitating international travel. Over the next five years, DHS will invest billions of dollars to modernize the passenger processes and systems inherited from the legacy agencies, including the US-VISIT system. Concerted efforts are now being made to realign certain operations and systems within the newly created DHS.

However, DHS did not conduct an analysis and reexamination of its strategy, processes, technology, and organization for the overall federal passenger processing requirements, i.e., business-process reengineering, before proceeding with US-VISIT. Further, DHS did not have an overall modernization acquisition strategy for the legacy Customs, INS, TSA, and APHIS systems related to passenger processing. An acquisition strategy based on a re-engineered vision of how DHS will process international travelers, in alignment with the department's enterprise architecture, should result in better and more definitive contract requirements.

We recommended that BTS initiate a business process reengineering effort to establish a clear vision of the overall federal operations that will be used to clear people entering and leaving the U.S., and based on the results, work with the Chief Acquisition Officer (CAO) and Chief Information Officer (CIO) to develop an overall departmental acquisition strategy for passenger information technology systems. BTS advised that it plans to initiate a business process reengineering effort, and develop an overall department acquisition strategy in coordination with the CAO and CIO.

Finally, in a report issued in June 2004, we raised concerns about the Secure Electronic Network for Travelers Rapid Inspection (SENTRI) program. This program permits pre-screened and enrolled low risk travelers to enter the U.S. from Mexico in designated lanes with minimal inspection by CBP officers, thereby avoiding the lengthy waiting

times in the regular inspection lanes. The SENTRI program is open to both U.S. citizens and certain non-citizens. We determined that the program is generally achieving the two basic objectives for which it was established: accelerating the passage of participating travelers through land ports of entry; and maintaining border integrity, security, and law enforcement responsibilities.

However, we noted inconsistencies in the way land ports of entry applied eligibility criteria for criminal offenses, financial solvency, and residency, and approved or denied applications. In addition, we noted weaknesses in the procedures by which SENTRI system records are kept current, and how alerts are disseminated to CBP officers. Taken as a whole, our findings indicate weak program management that could jeopardize the program's integrity and border security. In response to these concerns, CBP has moved to merge all of its trusted traveler programs and centralize the enrollment process to standardize enrollment procedures and criteria.

TRANSPORTATION SECURITY

DHS faces significant challenges in ensuring the security of the nation's transportation systems. TSA and the Coast Guard spearhead the department's transportation security efforts. While TSA has made progress in implementing the Aviation and Transportation Security Act (ATSA) and securing the nation's airways, improvements are still needed in aviation, rail, and transit security. Similarly, the Coast Guard has made progress in securing the nation's maritime transportation system, but the deteriorating condition of its aircraft and cutter fleets places the Coast Guard's current and future mission performance at risk.

Aviation Security

The success of TSA in fulfilling its aviation security mission depends heavily on the quality of its staff and the capability and reliability of the equipment to screen passengers and cargo to identify terrorists and terrorists' weapons, while minimizing disruption to public mobility and commerce.

Personnel. Providing qualified and trained personnel has been a substantial challenge for TSA. ATSA mandated that the TSA hire and train thousands of screeners for the nation's 429 commercial airports by November 19, 2002. As a result, TSA hired over 60,000 screeners. Our undercover audits of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not being carried into the sterile areas of heavily used airports, or do not enter the checked baggage system. Also, the ability of TSA screeners to stop prohibited items from being carried through the sterile areas of the airports fared no better than the performance of screeners prior to September 11, 2001. We attributed the test failures to four areas that were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA is enhancing its screener training programs along with management and supervision of screener activities. We are

currently evaluating TSA's revised training programs and will continue to monitor TSA's progress in improving screeners' performance. We plan to complete another round of undercover tests within the next 2 months.

Equipment. Providing capable and reliable equipment has also been a substantial challenge for TSA. TSA has been largely successful in its effort to implement the ATSA requirement that all checked bags be screened by explosives detection systems. However, deployment of the equipment does not ensure effective security. We reported that TSA has not resolved some of the problems that arise when explosive detection equipment breaks down, there are workforce shortages, or high baggage volume overloads the system. Fallback alternatives are inconsistently applied and inadequately controlled, leaving gaps in the screening process.

Furthermore, TSA has come under criticism for not moving quickly enough to address the vulnerability of the nation's air traffic to suicide bombers. For example, the 9-11 Commission recommended that TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. TSA is in the process of testing several of these technologies, including backscatter x-ray, vapor detection, and document scanner machines, to address concerns regarding detection of explosives on individuals. Until these advanced technologies are tested and deployed, TSA has instituted a process of more extensive pat-down procedures to find explosives hidden on a traveler. The use of these more thorough examination procedures have been protested by travelers and interest groups, and have already been refined by TSA. We are currently reviewing the implementation of these procedures to ensure they are strictly followed, as well as TSA's process for responding to passenger complaints.

TSA is currently piloting explosives trace detection document scanners at four airports to assess the viability and effectiveness of the technologies. We are monitoring TSA's progress regarding these issues as well as reviewing TSA's process for screening air cargo.

Rail and Transit Security

While TSA continues to address critical aviation security needs, it is moving slowly to improve security across the other modes of transportation. About 6,000 agencies provide transit services through buses, subways, ferries, and light-rail services to about 14 million Americans. Madrid's and Tokyo's terrorist experiences highlight potential vulnerabilities in transit systems. Recently, several congressional leaders expressed concern that the federal government has not taken strong enough action to respond to the threat to public transit. Furthermore, the 9/11 Commission reported that over 90% of the nation's \$5.3 billion annual investment in TSA goes to aviation, and that current efforts do not yet reflect a forward-looking strategic plan systematically analyzing assets, risks, costs, and benefits so that transportation security resources can be allocated to the greatest risks in a cost effective way. TSA's FY 2005 budget still focuses its resources on aviation.

TSA has lead responsibility for coordinating the development of a transportation sector plan, which is expected to be completed later this year. TSA, however, has not finalized the memoranda of understanding with various Department of Transportation agencies to determine how they will coordinate work in the future. We are evaluating TSA's actions to assess and address potential terrorist threats to the mass transit systems of major U.S. metropolitan areas.

Maritime Security

The Coast Guard's willingness to work hard and long hours, use innovative tactics, and work through partnerships in close inter-agency cooperation has allowed it to achieve mission performance results goals. However, to improve and sustain its mission performance in the future, the Coast Guard faces significant barriers, most importantly the deteriorating readiness of its fleet assets. The Coast Guard faces three major barriers to improving and sustaining its readiness to perform its legacy missions:

1. The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance.
2. The workload demands on the Coast Guard will continue to increase as it implements the Maritime Transportation Security Act of 2002 (MTSA). This complex work requires experienced and trained personnel; however, the Coast Guard has in recent years suffered from declining experience levels among its personnel.
3. Sustaining a high operating tempo due to growing homeland security demands, such as added port, waterway, and coastal security patrols, will tax the Coast Guard's infrastructure including its aging cutter and aircraft fleet.

The lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance. The Coast Guard has yet to define a performance management system that includes all the input, output, and outcomes needed to gauge results and target performance improvements, balance its missions, and ensure the capacity and readiness to respond to future crises or major terrorist attacks. For example, for search and rescue, the number of mariners in distress saved is a good indicator of outcome; however, resource hours under-represent the effort put into this mission by omitting the many hours of watch standing at stations. Without more complete information, the Coast Guard has limited ability to identify and target cost effective improvements to mission performance.

The workload demands on the Coast Guard will continue to increase as it implements the MTSA. Under MTSA, the Coast Guard must conduct risk assessments of all vessels and facilities on or near the water; develop national and area maritime transportation security plans; and approve port, facility, and vessel security plans. This complex work requires

experienced and trained personnel, presenting a major challenge for the Coast Guard, which has in recent years suffered from declining experience levels among its personnel. Since the Coast Guard largely relies on experienced senior personnel to coach and train junior personnel and new recruits on the job, mission performance is at risk.

In addition to implementing MTSA, growing homeland security demands, such as added port, waterway, and coastal security patrols, result in a continued high operating tempo. Sustaining this high operating tempo will be a major challenge for Coast Guard personnel and will tax its infrastructure, especially its aged cutter and aircraft fleet. The Coast Guard reported that mission sustainment is at risk due to cutters and aircraft that are aging, technologically obsolete, and require replacement and modernization. Currently, the Coast Guard is experiencing serious cracking in the hulls of the 110 foot cutters and engine power loss on the HH-65 Dolphin helicopters, resulting in operating restrictions. These problems adversely affect the Coast Guard's mission readiness and ultimately mission performance.

Maintaining and Replacing Deepwater Assets. In June 2002, the Coast Guard awarded a \$17 billion contract to Integrated Coast Guard Systems to maintain and replace its Deepwater assets. This contract called for replacing or modernizing, by 2022, all assets used in missions that primarily occur more than 50 miles offshore, including approximately 90 cutters, 200 aircraft, and assorted sensors and communications systems. According to the Coast Guard, the greatest threat to its ability to safely and effectively perform its assigned missions continues to be the operational capability of its legacy aircraft, cutter, and small boat fleet. These assets are aging and are becoming more expensive to maintain. In some instances, the Coast Guard is experiencing difficulty maintaining and upgrading existing critical deepwater legacy assets including the HH-65, HH-60, HC-130 aircraft, and its coastal patrol boat fleets.

As an example, the number of in-flight loss of power mishaps involving the HH-65 helicopter grew from about a dozen mishaps annually before September 11, 2001, to more than 150 in FY 2004, requiring the immediate re-engining of the entire HH-65 fleet. The Coast Guard recently accelerated its acquisition of the Multi-Mission Cutter Helicopter under development by the Integrated Deepwater System acquisition project, in addition to initiating engine replacement for its HH-65 helicopter fleet. Also, in 2003, the Coast Guard experienced 676 unscheduled maintenance days for its cutters—a 41% increase over 2002. This was the equivalent of losing the services of over three and a half cutters. These lost cutter days include the coastal patrol boats that are suffering from accelerated hull corrosion and breached hull casualties.

INTEGRATING THE DEPARTMENT'S COMPONENTS

Integrating its many separate components into a single, effective, efficient, and economical department remains one of DHS' biggest challenges. To meet this challenge, DHS, among other things, established an Operational Integration Staff to assist departmental leadership with the integration of certain DHS missions, operational

activities, and programs at the headquarters level and throughout the DHS regional structure

In any event, much remains to be done in integrating DHS programs and functions, and we have reported that structural and resource problems continue to inhibit progress in certain support functions. For example, while the department is trying to create integrated and streamlined support service functions, most of the critical support personnel are distributed throughout the components and are not directly accountable to the functional Line of Business (LOB) Chiefs, i.e., the Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Human Capital Officer (CHCO), Chief of Administrative Services (CAS), and Chief Procurement Officer (CPO).

In August 2004, the Secretary and Deputy Secretary directed the DHS LOB Chiefs to design and implement systems that will optimize their functions across the entire department. The LOB chiefs were also instructed to develop Management Directives to guide the department's management of those business functions. The Directives were to be built on a concept of "dual accountability," where both the operational leadership and the LOB chiefs are responsible for the successful preparation of the Directives and their ensuing implementation. This concept has been described as a "robust dotted line" relationship of agency or component functional heads to the LOB chiefs for both daily work and annual evaluation. Final Management Directives were signed by the Secretary in October 2004 to institutionalize the arrangements before FY 2005. In addition, the department's Management Council signed charters for each LOB that establish a formal governance and advisory board structure to ensure that the objectives and intent of the Directives are executed.

While the concept underlying the Management Directives may be workable in some environments, we have concerns that the DHS LOB chiefs may not have sufficient resources or authority to ensure that department-wide goals and challenges in their respective LOBs are addressed effectively, efficiently, or economically, or that available resources can be marshaled to address emerging problems. These concerns were heightened by the department's experience this past fiscal year in reorganizing the former Immigration and Naturalization Service (INS) and the U.S. Customs Service into three new bureaus – Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS), referred to as the "tri-bureaus" – and the consolidation of accounting services for many small programs from outside of DHS into ICE. However, the department and ICE did not prepare a thorough, well-designed plan to guide the transition of accounting responsibilities within ICE. ICE fell seriously behind in the performance of basic accounting functions, such as account reconciliations and analysis of abnormal balances. The pervasiveness of errors in ICE's accounts prevented the auditors from completing their work at ICE for the FY 2004 DHS financial statement audit.

The department also faces a structural problem in its financial management organization. The bureaus control most of DHS' accounting resources, but the DHS Chief Financial Officer (CFO) has responsibility for DHS' consolidated financial reporting, which is

dependent on those resources. Although coordination mechanisms are in place, monitoring controls at the DHS CFO's level are insufficient to ensure the accuracy of consolidated financial information. The seriousness of the material weaknesses and reportable conditions at DHS demands strong DHS CFO oversight and controls.

Similarly, creating a single infrastructure for effective communications and information exchange remains a major management challenge for DHS. We reported in July 2004, that the DHS CIO is not well positioned to meet the department's IT objectives. The CIO is not a member of the senior management team with authority to strategically manage department-wide technology assets and programs. No formal reporting relationship is in place between the DHS CIO and the CIOs of major component organizations, which hinders department-wide support for his central IT direction. Further, the CIO has limited staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support departmental units. These deficiencies in the IT organizational structure are exemplified by the CIO's lack of oversight and control of all DHS' IT investment decision-making and a reliance instead on cooperation and coordination within DHS' CIO Council¹ to accomplish department-wide IT integration and consolidation objectives. The department would benefit from following the successful examples of other federal agencies in positioning their CIOs with the authority and influence needed to guide executive decisions on department-wide IT investments and strategies.

We will be monitoring and evaluating the progress made in each LOB area very closely, not only during FY 2005, but also for years to come.

INTELLIGENCE

Under the Homeland Security Act of 2002,² the department is responsible for receiving, integrating, and coordinating the sharing of federal information to help ensure border security and protect the U.S. from terrorist threats. Specifically, the Homeland Security Act of 2002 gave DHS significant responsibility to coordinate the sharing of information to protect the U.S. from terrorist threats. The law requires the DHS Under Secretary for Information Analysis and Infrastructure Protection (IAIP) to consult with the Director of Central Intelligence and other appropriate intelligence, law enforcement, or other elements of the federal government to establish collection priorities and strategies for information relating to threats of terrorism against the U.S.³ The law also directs the IAIP Under Secretary to review, analyze, and make recommendations to improve the policies and procedures governing the sharing of law enforcement, intelligence,⁴ intelligence-related, and other information relating to homeland security.⁴

¹ The DHS CIO Council is comprised of the CIOs from each DHS component, ex officio representatives from General Counsel, the Chief Financial Officer's Council, the Office of the CIO, and the Executive Procurement Executive Council. The CIO Council was chartered to develop, promulgate, implement, and manage a vision and direction for information resources and telecommunications management within DHS.

² Public Law 107-296 (Nov. 25, 2002), codified at 6 USC 101 *et seq.*

³ 6 USC 121 (d)(10).

⁴ 6 USC 121 (d)(8).

However, with the creation of the Terrorist Threat Integration Center under the Director of Central Intelligence and the Terrorist Screening Center under the Director of the FBI, the role and responsibilities of IAIP for intelligence collection, analysis, and dissemination has been abated. Creation of the new Director of National Intelligence position makes the DHS intelligence coordination role even more uncertain, calling for prompt clarification of federal lines of authority in this area.

In a recent memorandum, the IAIP Under Secretary provided us an update on several actions being taken, which he believes will largely clarify some of these issues. Specifically, the IAIP Under Secretary said that the department has been fully supportive and involved in the development of a *Terrorist-Related Screening Procedures Strategy Report*, and a *Terrorist-Related Screening Procedures Investment and Implementation Plan* pursuant to Homeland Security Presidential Directive -- 11.

The recommendations from the strategy report were forwarded to the President in November 2004. The end result of such actions, the IAIP Under Secretary concluded, would be intra-agency watch list coordination and consolidation, a high-level review of terrorist information sharing activities, and a cohesive and coordinated federal screening program. We will continue to monitor progress in carrying out these activities to determine the extent to which they provide for a cohesive and coordinated federal screening and information sharing program.

PREPAREDNESS

Our office focused, so far, on examining the programs and mechanisms that enhance preparedness at the federal, state, and local levels of government, including the utility of IAIP data on port security grant award decisions. In its December 2004 report, the Heritage Foundation recommended consolidating DHS critical infrastructure protection, preparedness, and state/local/private coordination efforts under an Undersecretary for Protection and Preparedness. According to the Foundation, consolidating these disparate efforts would provide the DHS Secretary with a stronger platform from which to lead national efforts, determine priorities, identify critical vulnerabilities, work with state/local/private sector entities on securing those vulnerabilities and preparing for attacks, and make grants to help get the job done and to induce cooperation. Again, on the surface, this proposal appears to have merit. However, insofar as we have not studied the implications of this proposal, we are not in a position to address the pros and cons of such a consolidation. Nevertheless, we do have reservations about segregating FEMA's preparedness functions from its response and recovery responsibilities. Disaster preparedness, response, and recovery are intricately related, each relying on the other for success. This proposal should be carefully studied before it is put into practice.

Infrastructure Protection

One of the significant challenges facing the new Secretary is the need to base the department's business decisions, such as its grant awards, on information relating to nationally critical infrastructure and key assets. We learned from two surveys completed in 2004 and a more recent review of DHS' Port Security Grant Program, which we will issue shortly, that the department lags in integrating critical asset data and its "preparedness" initiatives into its business decisions. Also in 2004, we concluded that if IAIP did not produce a condensed list of most sensitive critical assets, other elements within DHS would be at risk of failing to direct their grant resources toward national critical infrastructure protection and preparedness. This concern materialized in port security grant awards: administrators designed and operated the program as a sector-specific grant program and conducted at least three rounds of grants, totaling \$560 million, without definitive national priorities for securing the seaport infrastructure of the nation. Poor integration of critical asset information meant that port security grant award decisions were made without sufficient information about our national priorities. DHS components need to strengthen their working relationships with IAIP, which has primary responsibility within DHS for critical asset identification, prioritization, and protection. The department's investments in new technologies, systems, and grant-making programs must reflect national priorities as determined by IAIP's risk management activities.

Also, a lack of coordination between the Science and Technology Directorate (S&T) and other DHS components slowed S&T's long term plan to invest in threat vulnerability and risk assessment tools. S&T is required to coordinate with other executive agencies, particularly those within DHS, to (1) develop an integrated national policy and strategic plan for identifying and procuring new technologies, (2) reduce duplication and identify unmet needs, and (3) support IAIP in assessing and testing homeland security vulnerabilities and possible threats. TSA, the Coast Guard, and IAIP have developed risk assessment tools and performed analyses of critical infrastructure. It is critical for the S&T to have a clear understanding of the terrorist threat picture facing the nation and the current technical capabilities and ongoing research and development initiatives of other DHS elements. To be effective, it must be able to prioritize its investment decisions, and avoid duplicating technology initiatives by other DHS components, especially in the area of risk assessment. To that end, the extent that the new Secretary oversees these efforts and makes intra-agency coordination a reality, will determine his effectiveness in ensuring that DHS' investments are adequately matched to risk.

We are seeing signs that IAIP is becoming more involved in risk assessment activity and grant decision-making across the department and agencies are increasingly seeking assistance from IAIP. S&T has intensified efforts to obtain terrorist threat information from IAIP and incorporate it into S&T's selection of new technologies. The Coast Guard is working closer with IAIP on maritime risk assessments and programs. Grant officials signaled their intention to consult IAIP and make better use of critical infrastructure information in future rounds of port security grants.

The new Secretary needs to ensure that this progress continues and becomes a regularized part of DHS's business decision-making. DHS components must share information, assimilate data to better coordinate risk management activities, and subscribe to a single concept of national priorities and interests. These actions are the foundation of solid business judgments now and in the future. Without this leadership, DHS risks having multiple, confusing, and possibly conflicting sources of priority for its investments.

State and Local Grant Programs

In March 2004, we reported on the distribution and expenditure of grant funds targeted for "first responders" in state and local jurisdictions. We reported that a slow rate of expenditure was due primarily to delays at the state and local level. In some cases, grantees delayed spending funds until they completed risk and strategy assessments that would enable them to spend the money more effectively.

We are currently reviewing preparedness issues through a series of ongoing audits. We are reviewing the effectiveness of state homeland security risk assessment and preparedness strategy processes. We are also reviewing the National Response Plan, to determine whether DHS has fully coordinated the National Response Plan with its state and local government and private sector partners; the plan meets the expectations of an all-hazards all-disciplines plan; and training and exercises are sufficient to fully implement the plan. Further, since July 2004, an OIG team has worked with DHS on a review of TOPOFF-3, the third and much expanded preparedness and response exercise involving top federal, state, and local officials and first responders.

We are also reviewing the Urban Search and Rescue Response System Preparedness Program. The objectives of this audit are to determine whether: the system's defined goals that relate to preparedness are being achieved; preparedness funding is having the intended effect on the system's capacity to respond to major disasters or emergencies; and there are opportunities for improvements in the program.

Finally, we are auditing state and local spending of First Responder Grant Funds. Our audit will determine whether: state and local jurisdictions are spending their first responder grant funds according to regulations and grant requirements; controls are adequate to ensure proper spending of grant funds; and program goals are being achieved.

Madam Chairman, this concludes my prepared statement. I will be pleased to answer any questions you or the members may have.

#

Statement of Dr. James Jay Carafano
 Senior Research Fellow
 The Heritage Foundation

Before the Senate Committee on Homeland Security and Government Affairs

Chairwoman Collins and other distinguished Members of the committee, I am honored to testify before the Committee today.¹ Thank you for the opportunity to discuss the conclusions of the task force chaired by myself, on behalf of The Heritage Foundation, and David Heyman of The Center for Strategic and International Studies. The task force's report, *DHS 2.0: Rethinking the Department of Homeland Security*,² evaluated the department's capacity to fulfill its mandate as set out in the Homeland Security Act of 2002.

My comments today are an abbreviated version of my written testimony, which I hope will be included in the record. Today, I will focus on the key management and organizational challenges raised by the task force. I will address: 1) the report and how its recommendations were developed, 2) leadership principles that could be used to guide implementation of the report's recommendations and specific examples where they could be applied, and 3) next steps for the department and Congress.

The findings and recommendations of the task force can be found on The Heritage Foundation's web site at www.heritage.org/Research/HomelandDefense/sr02.cfm. The report includes a bibliography of the documents we found most useful in our research.

¹The Heritage Foundation is a public policy, research, and educational organization operating under Section 501(C)(3). It is privately supported, and receives no funds from any government at any level, nor does it perform any government or other contract work. The Heritage Foundation is the most broadly supported think tank in the United States. During 2003, it had more than 200,000 individual, foundation, and corporate supporters representing every state in the United States. Its 2003 income came from the following sources:

Individuals – 52%
 Foundations – 19 %
 Corporations – 8%
 Investment Income – 18%
 Publication Sales and Other – 3%

The top five corporate givers provided The Heritage Foundation with 5 percent of its 2003 income. The Heritage Foundation's books are audited annually by the national accounting firm of Deloitte & Touche. A list of major donors is available from The Heritage Foundation upon request. Members of The Heritage Foundation staff testify as individuals discussing their own independent research. The views expressed are their own, and do not reflect an institutional position for The Heritage Foundation or its board of trustees.

²The task force co-chairmen and participants would like to acknowledge the helpful support provided by the Center for the Study of the Presidency and the use of its online Homeland Security Database and Information Exchange Site, which facilitated the task force's deliberations. The site is located at www.thepresidency.org/hsdatabase.htm.

Why This Report? Why Now?

Before I discuss the report, I would like to share with the Committee our rationale for undertaking this study and why the task force feels it is imperative that issues concerning the management and organization of the Homeland Security Department receive prompt attention from Congress and the department's new leadership.

We have learned a lot since 9/11. Americans have had ample time to dwell on the challenges of protecting the nation against foreign threats in the 21st century and to review the efficacy of our response to these dangers. It is time to rethink the place of the Department of Homeland Security in this effort.

The Task Force began by assessing the effectiveness of the department. On November 25, 2002, the Homeland Security Act of 2002 transferred over 22 federal entities, some intact and some in part, and 180,000 employees into a single department—the Department of Homeland Security (DHS). A requirement to revisit the organization and management of the department should have been axiomatic. Complex mergers are bound to encounter resistance, unanticipated problems, and obstacles that can't be overcome without decisive intervention by the organization's leadership. Identifying these challenges and addressing them must be a priority.

Nor is it prudent to wait much longer to address management and organizational challenges. Experience reminds us that it takes only a few years for bureaucracies to become entrenched and virtually impossible to change. The creation of the Department of Defense is a case in point. In the debates over the 1947 National Security Act, and again, as President, Dwight Eisenhower lobbied for reorganizing the Pentagon to ensure that Army, Navy, Marine, and Air Force assets would work closely together. He failed to overcome the political opposition and the service parochialisms that blocked reforms. As a result, fundamental problems in joint operations went unaddressed until 1986 with the passage of the Goldwater–Nichols Act.³ The lesson is clear. Fix it at the beginning or live with the mistakes for a long time.

What We Did

A task force with members from academia, research centers, the private sector, and Congressional staff from both sides of the aisle and chaired by homeland security experts at The Heritage Foundation and The Center for Strategic and International Studies examined the effectiveness of the new department in four areas: management, roles and missions, authorities, and resources.

Based on this analysis, conducted through seminars, an extensive literature search, and interviews, the task force developed 40 major recommendations for improving the oversight, organization, and operation of DHS. We believe that, taken together, this

³James R. Locher III, *Victory on the Potomac: The Goldwater–Nichols Act Unifies the Pentagon* (College Station: Texas A&M University Press, 2002), pp. 25–31.

report makes the case for a significant reorganization of the department to empower the Secretary, and creates a more effective and efficient instrument for preventing and responding to terrorist threats.

The report is divided into four sections. Each one presents the conclusions of the task force. The sections address how well DHS is fulfilling its mandate as defined by the Homeland Security Act. The four areas are:

Management. Considers the organization and functions of the DHS secretariat and its capacity to integrate and effectively direct departmental activities and to provide a coherent vision for the future.

Roles and Missions. Presents findings and recommendations concerning the organization and conduct of operations for the department's most critical security tasks.

Authorities. Addresses the adequacy of the legal authorities and policies governing significant department activities.

Resources. Looks at limitations in the department's ability to efficiently and effectively allocate resources to respond to critical missions.

Each section consists of findings and recommendations agreed upon by the task force. The findings represent what we believe to be significant statements of fact that are affecting the department's performance. Recommendations are measures that the task force proposes be undertaken by the Administration and Congress to improve the organization and operation of the department. Major recommendations in the report include:

- **Strengthening** the Secretary of Homeland Security's policymaking function by creating an Undersecretary for Policy.
- **Empowering** the secretary by establishing a "flatter" organizational structure through: (1) consolidating and strengthening agencies with overlapping missions; (2) eliminating middle-management (directorate) layers over border and transportation security, preparedness and response, and information analysis and infrastructure protection; and (3) having the agencies report directly to the secretary via the Deputy Secretary of Homeland Security.
- **Rationalizing** government spending by establishing a risk-based mechanism for department-wide resource allocation and grantmaking and by developing pre-determined "response packages" to respond to catastrophic terrorism.
- **Clarifying** authorities and national leadership roles for bio-defense, cyberdefense, and critical infrastructure protection.
- **Improving** departmental oversight by rationalizing congressional committee structure and establishing permanent oversight committees in the House of Representatives and the Senate.

What We Learned

In retrospect, there are three principles that could guide implementing the report's recommendations. They are:

- **Make** reorganizing the management of the department a first priority;
- **Develop** a future vision of the department to guide further reorganization; and
- **Divide** department activities between operational responsibilities and support functions under different chains of command.

I will now discuss each of these in turn and use a specific challenge now facing the department and recommendations from our report to illustrate how the principles could be applied.

Focus on Management First

It is interesting to note that, in concert with the *DHS 2.0* report, the DHS Inspector General (IG) identified management as a significant issue. "Integrating its many separate components into a single, effective, efficient, and economical department," the IG wrote, "remains one of DHS' biggest challenges."⁴ As the IG report points out, the department lacks "horsepower" within the secretariat to set policies and programs department-wide. Critical support personnel are distributed throughout the department and not accountable to the chief officers (such as the Chief Information Officer) who are responsible for integrating and coordinating departmental functions. Nor do the chiefs have sufficient staff and resources.

The weaknesses in DHS management are critical because they cut against the core rationale for passing the Homeland Security Act of 2002—gaining the synergy of having most of the key federal agencies with homeland security responsibilities grouped in one department.

DHS attempts to "work around" these management challenges by relying on a concept called "dual accountability," where agency staff are asked to report both to the heads of their agencies and chief officers in the secretariat.⁵ Dual accountability can be a successful management process in mature organizations with well-established procedures, strong organizational cultures, and clear roles and missions. DHS lacks these kinds of formal institutions. DHS requires a cleaner management structure based on a chief-operating officer model and supported by staff organized and empowered to integrate activities department-wide.

The Problem of Policy

⁴Office of the Inspector General, "Major Management Challenges Facing the Department of Homeland Security," Department of Homeland Security, December 2004, p. 1.

⁵Office of the Inspector General, "Major Management Challenges, p. 2.

For example, improving the department's capacity to develop integrated policies is one area where there is a substantial need for better management. The DHS Secretary currently lacks a policy apparatus, from which to lead the development of proactive, strategic homeland security policy—let alone to anything beyond “managing by the inbox,” and responding to the crises of the day. DHS also currently lacks a high-level policy officer with staff, authority, and gravitas to articulate and enforce policy guidance throughout and across the department. DHS needs a more substantial capability to provide guidance for integrating current efforts.

When DHS was formed from dozens of existing U.S. government agencies and programs, it absorbed several legacy policy analysis units from its component agencies. In addition, the patent need for policy analysis led some DHS components to form their own small policy analysis units. The proliferation of policy centers within DHS has only magnified the challenge of forging coherent guidance.

Nowhere is the need for policy integration more apparent than in international affairs. Until recently, the Office of International Affairs (OIA) and the Department's Deputy Chief of Staff for Policy and—subsequent to her departure—an “Advisor to the Secretary for Policy” conducted parallel international affairs operations. Individuals from both offices called department-wide meetings to discuss international affairs; met with foreign government representatives; recommended scheduling of meetings for the Secretary with foreign officials; traveled internationally; drafted department-level documents for the Secretary's consideration on international issues; assumed the lead for international meetings, conferences, or trips by the Secretary; and participated in interagency meetings that addressed international issues. In most instances, OIA has been unaware of the international activities of individuals assigned to the Office of the Chief of Staff.

Among the international offices in each of the DHS directorates and separate agencies it is not clear where to look for international policy guidance. The Office of International Enforcement established within the Directorate of Border and Transportation Security is a case in point. The office, in conjunction with the Deputy Chief of Staff for Policy vetted options for restructuring the international affairs of the Department, excluding OIA from its deliberations.

Our report recommended establishing a unified policy planning staff, headed by an Under Secretary for Policy who would report directly to the Secretary via the Deputy. The Under Secretary would serve as the Secretary's chief policy official within the Department. The responsibilities of the Undersecretary for Policy should be established by law. The responsibilities for international affairs should be included in the secretariat. They should include:

- (1) *Coordinate DHS policy.* The Under Secretary would establish and direct a formal policymaking process for the department and oversee a Policy Making Board;
- (2) *Conduct long-range policy planning.* The Under Secretary's staff would conduct long-range strategic planning, including “what-if” scenario-based planning—a

task other DHS components invariably neglect as they grapple with daily crises and other pressing short-term demands;

- (3) *Prepare critical strategic documents*, such as a strategy for preventing terrorists for entering the United States. The Under Secretary's office would help compose the department's most important documents;
- (4) *Conduct program analysis*. The Under Secretary would assist with DHS programming. In particular, his or her analysts would evaluate ongoing and proposed programs (including planned research and development efforts) in terms of overall DHS priorities and resources; and
- (5) *Prepare net assessments*. The Under Secretary's planners would conduct periodic net assessments and research specific issues of interest to the Secretary and other DHS leaders that cut across the department's components or for which the leadership desires another opinion.

As part of this reorganization the law should convert the position of the Office of International Affairs Director to an assistant secretary under the Under Secretary for Policy, eliminating the redundancy of roles between the Chief of Staff's office and OIA, and realigning all DHS-wide international policymaking activity under an undersecretary. The law should clearly delineate the key responsibilities of the Assistant Secretary for Policy (International Affairs). They should include: (1) Coordinating policy regarding international activities among the DHS agencies; (2) Coordinating international visits of the secretary related to protocol issues; and (3) Ensuring DHS representation in dealing with international institutions, including the United Nations, NATO, the EU, the International Maritime Organization, and the World Customs Organization.

Focusing on management first, reorganizing the secretariat so that it could more effectively integrate department-wide activities such as policymaking and international affairs, is a prerequisite for improving the performance of DHS.

Envisioning the Future

One hotly debated issue relates to the division of roles and missions within the department. The creation of DHS was supposed to consolidate agencies with overlapping missions. Since its formation, DHS has made some positive efforts to group the right activities under the right organization. Moving the Office of Air and Maritime Interdiction under Customs and Border Protection (CBP) and shifting the Federal Marshal Service to Immigration and Customs Enforcement (ICE) are cases in point. However, a broader assessment needs to be made across the department.

There is reluctance to undertake such a review based on the argument that the organizations have not yet absorbed all the changes heaped upon them. Such thinking is shortsighted. DHS needs to be constructed not to accommodate the present, but to build toward the ideal organization of the future. Therefore, DHS needs to articulate how it envisions conducting its missions five to ten years from now and let this vision drive the organizational design.

One Face at the Border and Beyond?

How DHS should structure to address border, transportation, and internal customs and immigration enforcement offers a case where there is serious need to “envision the future” and use that vision to drive reorganization. In “consolidating” responsibility for border, immigration, and transportation security, DHS actually increased the number of involved agencies to eight and created more problems that now need solving. In addition, it has failed to clearly delineate the missions of agencies within DHS that also have border, immigration, or transportation security responsibilities.

In particular, the split of responsibilities between Customs and Border Protection and Immigration and Customs Enforcement was done without a compelling reason—other than the vague descriptive notion that CBP would handle “border enforcement,” and ICE would handle “interior enforcement.” Indeed, in various interviews, not one person has been able to coherently argue why CBP and ICE were created as separate operational agencies.

The proposal in our report would rationalize border security and immigration enforcement by merging CBP and ICE eliminating the Directorate of Border and Transportation Security (BTS). BTS has neither the staff nor infrastructure to integrate the operations of CBP and ICE on a consistent basis—outside the occasional task force, like the Arizona Border Control Initiative. Nor does it have a policy operation with sufficient influence with the Secretary to resolve policy conflict. Merging CBP and ICE will bring together under one roof all of the tools of effective border and immigration enforcement: Inspectors, Border Patrol Agents, Special Agents, Detention and Removal Officers, and Intelligence Analysts—and realize the objective of creating a single border and immigration enforcement agency.

Whether this specific recommendation makes sense or not depends in large part on the department’s vision for controlling the border and enforcing immigration laws over the next decade. Once DHS articulates its long-term strategy for how it plans to fulfill its functional responsibilities, it will be prepared to address the need for further consolidation and reorganization. Envisioning the future could be an important tool for determining the most efficient division of roles and missions within the department.

Divide Responsibilities

In reviewing the task force’s recommendations, it is apparent that our proposals evolved into an effort to divide functional responsibilities in the department between “operational” agencies (e.g., border control and interior enforcement) and “support” staff and directorates (e.g., planning, policy, and acquisition). This is a sound management principle because it focuses agencies on a critical mission, rather than trying to do everything. The Defense Department explicitly follows this model. Combatant commanders are charged with “running the war.” The services are responsible “raising, training, preparing, and sustaining” the force. It is a model that works well because it encourages organizations to focus on their core competencies.

Preparedness, Protection, Response—Drawing the Line

Nowhere is their greater need to rethink how responsibilities are divided than in the missions of protection, preparedness, and response. In practice, protection and preparedness are “support” functions. Response is an “operational” function. Yet, DHS has divided these responsibilities “helter skelter” throughout the department. The ability of the DHS Secretary to lead is hampered by the fragmentation of key responsibilities at least eight entities:

- (1) The DHS Emergency Preparedness & Response (EP&R) Directorate. This Directorate is primarily the Federal Emergency Management Agency (FEMA), but it also includes within it certain efforts to coordinate with state, local, and private entities on preparing for disasters, including terrorist attacks;
- (2) The Infrastructure Protection (IP) piece of the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate. The job of IP is to identify critical infrastructure warranting protection, prioritize efforts, and work with state, local, and private entities to secure this infrastructure. Within the IP subdirectorate is the office in charge of cybersecurity;
- (3) The DHS Office of State and Local Government Coordination and Preparedness (OSLGCP). This entity—the product of merging the Office of State and Local Coordination, and the Office of Domestic Preparedness—works with state and local governments on identifying needs, coordinating efforts, and doling out DHS grant money for critical infrastructure protection and preparedness;
- (4) Transportation Security Administration (TSA);
- (5) The U.S. Coast Guard. In addition to its operational responsibilities, the Coast Guard is also responsible for protecting seaports through risk assessments, reviewing facility security plans, developing Area Maritime Security Plans, coordinating Area Maritime Security Committees, and facilitating Port Security Grants with the Maritime Administration. The Coast Guard also has Maritime Safety and Security Teams, and Strike Teams, to respond to incidents at the ports;
- (6) Office of Private Sector Liaison. This office has primarily been an ombudsman for private efforts to influence DHS policy in various areas, but it conceivably could be a forum for working with the private sector on critical infrastructure protection and preparedness for attacks;
- (7) DHS Science and Technology Directorate Office of WMD Operations and Incident Management (WMDO-IM). This new office, within the S&T Directorate, is intended to provide rapid scientific and technical expertise and decisionmaking in response to WMD attacks and incidents;
- (8) Department of Health and Human Services—Assistant Secretary for Public Health Emergency Preparedness, and the Centers for Disease Control (CDC). These agencies outside DHS are central to our ability to prepare for and respond to a bioterrorism attack.

Meshing operational and support functions in one agency, as is the case in FEMA illustrates the problem. For example, in September the FEMA preparedness office in

Emmitsburg, Maryland had planned a conference for all its regional directors. The FEMA response to the hurricanes in Florida required canceling the meeting because preparedness personnel had to be deployed to supplement response personnel. A similar situation occurred after the September 11 attacks: By some accounts FEMA cancelled all preparedness activities for the next six months. Changes in operational tempo should not bring a halt to national preparedness activities. Yet, that is what normally happens in organizations where “here and now requirements” take priority and trump other actions. In such organizations, “peripheral” non-operational activities never receive adequate priority.

The fragmentation of DHS leadership efforts into discrete—and often competing—agencies hampers efficiency. While the task force did not recommend the transfer of agencies from outside DHS given the important interrelationships with their home Departments (e.g., the interrelationship between the Assistant Secretary of HHS for Public Health Emergency Preparedness with broader public health issues), we do advocate—at a minimum—further consolidations within DHS, to unify and focus DHS efforts and enable the Secretary to work effectively with other departments on the critical national priorities of securing critical infrastructure, preparing for terrorist attacks, and responding to them.

The recommendation of the *DHS 2.0* report is to consolidate DHS critical infrastructure protection, preparedness, and State/Local/Private coordination efforts under an Undersecretary for Protection and Preparedness. This would consolidate the following agencies: (1) the Infrastructure Protection component of the Information Analysis and Infrastructure Protection Directorate; (2) Office of State and Local Government Coordination and Preparedness (OSLGCP); (3) the non-operational transportation infrastructure protection mission of TSA; (4) the “preparedness” piece of the EP&R Directorate; (5) the private sector preparedness mission of the Office of Private Sector Liaison; and (6) grantmaking authority for the DHS. Consolidating these disparate efforts would provide the DHS Secretary with a stronger platform from which to lead national efforts, determine priorities, identify critical vulnerabilities, work with state/local/private sector entities on securing those vulnerabilities and preparing for attacks, empower them to make grants to help get the job done, and induce cooperation.

Additionally, the task force recommended focusing all DHS “response” missions into FEMA, and strengthening the agency. FEMA should be engaged squarely in its traditional role of planning for the national (not just federal) response to emergencies, including terrorist attacks, and then implementing them where necessary. Likewise, the task force proposed eliminating the EP&R Directorate. Both the proposed Undersecretary for Protection and Preparedness and FEMA should report directly to the secretary via the deputy.

Consolidating operational efforts renders unnecessary the “middle management” directorate layer. Meanwhile grouping support functions under authorities like the Undersecretary for Protection and Preparedness will help consolidate support activities throughout the department. In both cases, efforts to divide responsibilities and establish

centers of competency and excellence along functional lines should enhance the effectiveness of DHS.

Where Do We Go From Here

Our report called for the President and Congress to establish a non-partisan commission to review the performance of the department and assess its capacity to fulfill the missions outlined in the Homeland Security Act and report back within six months. Without permanent oversight committees in the Senate and House, we felt Congress would be unable to effectively address the challenge of restructuring DHS. Things have changed. The Task Force applauds the action taken in both chambers to create permanent committees. With Congressional oversight of the department's management now consolidated in appropriate committees, Congress could consider alternative paths for moving forward. One would have Congress move now to legislate key management reforms and establish a routine authorization process and then address rethinking roles and missions, authorities, and resources in a more deliberate manner through a combination of reviews conducted by DHS and an independent panel answering to Congress. This strategy might proceed as follows:

Step #1. Legislate Undersecretaries for Policy and Protection and Preparedness and abolish the Undersecretary for Emergency Preparedness and Response. Establish Chief Operating Officer functions under the Deputy Secretary.

Step #2. Implement an Authorization Process for DHS. An authorization bill for DHS could serve as a critical statutory management tool providing means to exercise stronger oversight of important DHS activities such as key personnel programs, performance of critical missions, major research programs, and information technology investments.

Step #3. Establish a Requirement for Periodic Reviews. Congress should establish a requirement for DHS to conduct quadrennial reviews to access the department's strategies, force structure, resources, and appreciation of the threat. The Quadrennial Homeland Security Review (QSR) should be timed to coincide with the mid-point of the presidential term. The first QSR should be specifically tasked to address roles and missions, authorities, and resources.

Step #4. Create a one-time National Homeland Security Panel. In parallel with the first QSR, the Congress should establish a non-partisan National Security Review Panel (NSP). The NSP should be charged with providing an independent assessment of the QSR as well as assessing the efforts of DHS in the context of larger national security programs and strategies.

Conclusion

DHS now faces the same challenges that confronted the Pentagon in 1947. In terms of efficiencies and improved coordination, the simple solution of corraling over 180,000 employees into one agency has been done. What remains is the hard work—implementing human capital, acquisition, and information technology programs; building

security systems that match the national strategy; and standing watch every day against terrorist attacks. Oversight of these activities requires an effective management structure within the department and the support and guidance of this committee. Now is the time for action.

Once again, thank you, Chairman Collins, and the rest of the Committee for holding this important hearing and for inviting me to participate. I look forward to answering any question you might have.

**Statement of Michael A. Wermuth¹
Director, Homeland Security
The RAND Corporation**

**Before the Committee on Homeland Security and Governmental Affairs
United States Senate**

January 26, 2005

Madam Chair, Mr. Ranking Member, and distinguished Committee Members, thank you for giving me the opportunity to appear before you today, to address the important issue of ways to improve the security of our homeland.

My remarks today will be informed in great measure by relevant and comprehensive research and analysis conducted by the RAND Corporation over many years. It includes the major areas of research and analysis to support the deliberations and recommendations of the congressionally mandated Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (also known as the “Gilmore Commission”)², over the course of its five annual reports to the President and the Congress from 1999 to 2004.

My remarks are also based on significant research on related matters for the White House Office of Homeland Security, the Department of Homeland Security, the Department of Justice (including the Federal Bureau of Investigation), numerous entities within the Department of Defense, various agencies of the Intelligence Community, the Department of State, the Department of Health and Human Services, the Department of Energy, the Department of Transportation, and several other federal departments and agencies. It likewise includes related

¹ The opinions and conclusions expressed in this testimony are the author’s alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND’s publications do not necessarily reflect the opinions of its research clients and sponsors.

² Established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261 (H.R. 3616, 105th Congress, 2nd Session)(October 17, 1998), as amended.

research and analysis for various agencies of the State of California, the State of Georgia, the City of New York City, other State and local entities, as well as research commissioned by private foundations and others.

In addition—as you may well imagine—I also have some opinions on current issues for which there may not be current or related RAND research. I will do my best to separate evidence supported by our extensive research and “opinion” evidence.

Please let me also acknowledge the key leadership of the Chair and Ranking Member on these issues, not only your instrumental role in the passage of the Homeland Security Act of 2002, and the Collins-Lieberman Intelligence Reform and Terrorism Prevention Act, signed by the President just a little over a month ago, but on numerous other related legislative initiatives. Few others on either side of Capitol Hill can claim anything like the level of dedication and commitment you have shown in securing our homeland.

You have asked that this testimony address the primary management challenges faced by the Department of Homeland Security (DHS) and to describe those challenges as they have impacted the Department’s efforts on border security, transportation security, emergency preparedness and response, and intelligence. Within the context of those functional areas, I will discuss six critical challenges facing DHS. Four of them are issues that DHS itself will have a strong role in resolving; two are challenges that DHS cannot directly control and instead must call on the President and the Congress for assistance. The first challenge is the lack of robust strategic planning and analysis capabilities in the Department. This deficiency is clearly revealed in the context of border and transportation security and in other areas as well. The second major challenge is the lack of performance metrics and the inability to tell what works and what doesn’t. Though this problem applies broadly across the Department, today I will

illustrate its impact in the realm of transportation security. The third challenge is the structure of the organization, both internally and as it relates to other organizations. Again, although this problem applies broadly across the Department, I will demonstrate the impact in only a couple of areas. The fourth problem is intelligence, as it relates to the fulfillment of the DHS operational mission, from the standpoint both of what DHS does internally and from the part external actors must play in the intelligence process. The last two are almost entirely “external” to DHS and have to do with both obligations and some missed opportunities in areas of strategic guidance and oversight on the part of the White House and the Congress.

Border Security

It is my personal opinion that perhaps the greatest advances made in homeland security after September 11, 2001, are in the border security arena. Clearly, much remains to be done. The structures and processes already in place have added in a measurable way to the attempts to prevent those who would seek to do us harm from entering or remaining in the United States. But much remains to be done. This remains a very complicated arena and security in and of itself cannot be the only consideration.

Our border security efforts have significant and direct impact not only on our own domestic economy but on the global economy. There are significant diplomatic, political, and societal implications to be considered. The staging, sequencing, and enforcement methods at our borders require a broader, more holistic view of the problem.

As one cogent example, in our global economy, the U.S. is dependent on a variety of supply chains of goods and resources from all over the world, one that was not created with security at its core. Those supply chains involve major interests at several different levels—various government agencies (domestic and international); the global transportation and

communications networks; and suppliers, marketers, and users in many parts of the chains as well as the significant movement of people in connection with those supply chains. There is, as yet, no comprehensive approach to address all the various aspects of supply chains not only in security terms, but also the impacts that security or the lack thereof can have on economies, diplomacy, governmental stability, societal well-being, and much more. RAND has recently completed and published a report entitled *Evaluating the Security of the Global Containerized Supply Chain*, which reflects in its analysis of that issue the need for a more holistic approach to the entire spectrum of supply chain matters. We ask that this report be part of the record of today's hearing.

To support strategic, holistic approaches to such issues, we are in full agreement with others who have made similar recommendations that the department needs a robust capability to engage in long-range strategic thinking leading to the refinement or development of strategies, policies, and implementation plans—on a department-wide basis—rather than the somewhat fragmented approach that currently exists. We would suggest that the entity be an Under Secretariat for Policy *and* Planning to make it clear that its responsibilities include both important and different functions. We know that current senior leaders in DHS favor such a change and that there is fairly broad support for that proposition on the Hill.

The importance of long-range strategic planning cannot be overemphasized. As we get better with security at the designated official points of entry, we will push terrorists and other criminal enterprises to unregulated points—areas that are by their geophysical nature difficult to regulate. But we must have a system in place to consider these second-order effects and develop plans that are flexible to meet changing threats.

We have been asked to comment on recommendations for organizational changes in the border security structures, such as the merger of bureaus for Customs and Border Protection (CBP) and Immigrations and Customs Enforcement (ICE). Madam Chair and Members, it may not be the answer others are looking for, but we are not yet convinced that such a move is necessarily indicated and would be more effective. That opinion is based on a long history of doing organizational research and analysis for numerous government clients. Consider, if you will, that CBP and ICE do in fact have fairly disparate functions. CBP is the entity that, through its inspectors, performs ministerial—albeit important ministerial—functions leading up to and at our border points of entry. Those functions include the routine check of advance passenger manifests, passports, and visas as well as the review of advance cargo manifests for determination and collections of customs duties and fees as well as the identification of potential contraband. ICE on the other hand performs, through its investigators—sworn federal “1811” officers—critical law enforcement functions to identify, through a variety of sources, those who would attempt to circumvent customs or immigration requirements or otherwise break U.S. laws—for example, the importation of illegal drugs and other contraband—and often in cooperation with other agencies arrest perpetrators and seize illegal goods. Given those different functions, a good argument can be made that the skills required for the performance of those separate tasks require different recruiting, retention, training, performance evaluation, operational procedures, and other related activities. It could be that rushing into such a change without further study—comprehensive analysis of all the issues, structures, and dynamics involved—will not be result in the intended consequences of more efficient and effective border security. There are some useful analogies. One is a military parallel: combat units are different than combat support and combat service support units. The skill sets and therefore the training

and personnel systems are different. Another example worth considering is the fact that, many years ago, Congress decided to create a Drug Enforcement Administration—separate from other federal law enforcement agencies—in order to focus on that critical activity. That is not to say that, even for the military or DEA, such different types of commands or agencies are not required to maintain close coordination with counterpart organizations; surely they must. And the same holds true for CBP and ICE. But for this issue and other major reorganization recommendations, contained in reports such as the Heritage Foundation-Center for Strategic and International Studies joint report “DHS 2.0” and others, we advise against making some of those dramatic changes without further and comprehensive analysis of the impact.

Madam Chair and Members, I know what I am suggesting is hard work but it is important work that should be done.

Transportation Security

As is the case for border security, in the area of transportation security, there must, and we argue can be, more holistic approaches that cut across old bureaucratic lines and various missions and functions.

We believe that it is essential to move more toward a “risk management” approach to decisionmaking, including better prioritization for resource allocation and the development of future strategies, plans, and programs based on that risk management approach. Again this is why we support the creation of an Under Secretariat for Policy and Planning.

A case in point is the roles and missions of the Transportation Security Administration (TSA). TSA should be tasked only for operational missions and not policy development, other than those purely internal TSA policies required to perform its operational missions.

Transportation security writ large is broader than just TSA and should be informed by the development of policy and planning at the department level.

There are many other examples to amplify on the requirement for more strategic, holistic policy and planning approaches, but I'll mention only a couple. Today, RAND is releasing a report on defending our commercial airline fleet against attacks using shoulder-fired missiles. That report concludes that it is currently not cost-effective to spend some tens of billions of dollars equipping America's 6,800 commercial airliners with systems to guard against this threat, but investment could be justified in the future if anti-missile systems are made more economical and reliable. Installing such systems on the nation's fleet of commercial airliners would cost an estimated \$11 billion, with operating costs ramping up to \$2.1 billion annually upon full operational capability, according to the RAND report. Over 20 years, the cost to develop, procure and operate these systems would amount to an estimated \$40 billion. By way of comparison, the federal government currently spends about \$4.4 billion annually on all transportation security. We have sent electronic copies of this new report to the Committee staff in preparation for the hearing and we now ask that the report be included in the record of today's hearing.

I am also frequently asked whether we are doing enough, spending enough, on rail security. The simple answer is that we cannot know without a thorough analysis of many factors.

Better, more comprehensive, more authoritative measures of performance and effectiveness—a valid metrics program for homeland security activities and investments—must be developed and implemented. The primary measure of effectiveness or performance cannot continue to be the level of expenditures on a particular activity. A truly valid metrics program

will include clearly identified targets for specific performance at designated points on timelines or other proven techniques for evaluation the effectiveness of resource expenditure and other criteria. Comprehensive accountability criteria must be established that can be audited and assessed to ensure the most effective use of scarce resources. Once again, not easy tasks but essential ones, and is it here that a new Under Secretariat for Policy and Planning can add great value.

For the structural side of transportation security, on the same rationale expressed above in connection with any proposal to merge CBP and ICE, it is not clear—without much further analysis and debate—that it would necessarily be more effective to eliminate the Border and Transportation Security Under Secretariat and have the “operational” entities report directly to the Secretary through the Deputy. There are important span-of-control considerations. To use a military analogy, such a recommendation is tantamount to suggesting that all Army Divisions engaged in a major military operation should report directly to the most senior commander and that Army Corps headquarters can be eliminated.

By the same token, it is clear that the BTS directorate, if retained, must be appropriately resourced to perform the integration of the operational entities subordinate to that structure.

Emergency Preparedness and Response

Madam Chairman and Members, I will address the emergency preparedness and response management challenges from both a DHS internal and external perspective. Existing structures may not work, and thorough analysis is required to determine if new models are better. Moreover, DHS cannot be like many other federal bureaucracies; it must have tighter geographic links to the “field” for closer coordination with states and localities, and more comprehensive collaborative arrangements with other federal “partners.”

Internally, the Emergency Preparedness and Response (EP&R) Under Secretariat is little more than FEMA with a few extra “front office” personnel. Over the course of its existence, FEMA has had an inconsistent record of effectiveness, engendered, at various times, from leadership issues, resource problems, and other matters.

There may, in fact, be valid constructs that should be considered other than one to eliminate EP&R and consolidate other programs into FEMA. In the post-September 11 environment, with major new initiatives in both preparedness and response-some of which are well outside traditional FEMA missions for disaster response and recovery, it may be useful to do a complete top-to-bottom analysis of FEMA and EP&R juxtaposed with the requirements of this new environment. That analysis could consider, among other things, actual splitting FEMA into two separate parts-one for preparedness functions and one for post-event response functions-as an alternative to collapsing other functions into the existing FEMA. For the same span-of-control issues noted above in the border and transportation security discussions, alternative analyses of EP&R should include its retention and division into separate subordinate entities-one for preparedness and one for response-with the integration of other DHS preparedness and response functions into the respective divisions. There may be other approaches as well, and each should be considered in a thorough analysis.

Now for the external side of emergency preparedness and response: for starters, DHS should move quickly to implement its regional structure. Given the critical importance of closer cooperation with states and localities, and the acknowledged differences in preparedness and response issues based on U.S. geographical diversity, it is time to put some new structure in place even if it needs to be changed later based on actual experience, on lessons learned subsequently. That structure, along with the publication of the National Incident Management

System last year and the recent release of the full National Response Plan, will provide opportunities to test and evaluate various aspects of this structure and identify further refinements and required improvements in many areas, including research and development and future resource allocation.

There are other significant external preparedness and response considerations. RAND has noted in various reports and other research products that there are other needed improvements in the structures and processes for coordination and potential joint operations between DHS and numerous other federal entities as well as states and localities, potentially foreign governments and domestic and foreign private sector organizations.

Let me offer one important example at the federal level: the need for the development of more formal relationships between DHS and the Department of Defense (DoD). First, DoD will likely be called upon again—as it has been on so many occasions for natural disasters and other situations—to provide what is now known as Defense Support to Civil Authorities. We believe more work can be done that will allow DoD to respond more effectively. And DHS should, in coordination with DoD, be responsible for leading that effort. We will call it the Requirements Generation Process. DHS has the responsibility by statute to be the focal point for requests for support that may start at the local level and come up through a Governor to the federal level. DHS needs to create a mechanism in which states, and through them localities, will be required to provide an estimate of required federal support based on a variety of scenarios. That is not a process that DoD should undertake alone, although, in the absence of DHS doing it, that is exactly what is happening to a certain extent. When an incident occurs that may require DoD support to a state or locality, that request for support will not go directly to the Secretary of Defense; it will go to DHS for validation and a determination of appropriate federal support,

perhaps including DoD. How can DHS adequately perform its function for validating support requests from states if it is not involved in the front end of the requirements process?

And there is a flip side to this issue. It is now widely recognized that there are potential “homeland defense” missions, something arguably distinguishable from other homeland security missions, where DoD actually has the “lead” for the federal government. One good example comes from September 11 itself. A fourth hijacked plane was still in the air after the attacks in New York and at the Pentagon, when Air Force fighters were launched in an attempt to intercept. Except for the intervention of passengers on that flight, if that plane had been located, it may well have been shot down. Those on the ground responding to such an incident were and would not be military personnel but civilian local responders. The same could hold true for homeland defense operations in maritime regions, even potentially along land borders or other land areas. Does that not indicate that more thought, discussion, coordination, and planning for “Civil Support to Military Authorities” would be a good idea?

In addition, there continues to be a need for comprehensive debate and decision on the appropriate role of the National Guard in homeland security, homeland defense, and foreign missions. That is, of course, not directly within the scope of this hearing but should, I suggest, be undertaken in more deliberate fashion by the Congress.

Intelligence

No other issue has captured more of center stage in the discussions of homeland security than the acknowledged shortcomings pre-September 11, in the structures, processes, and operations for the collection, analysis, and dissemination of intelligence related to the security of our homeland. Thanks in great measure to the leadership of the Chair and Ranking Member, we now have some legislatively-mandated new structures and processes in place to address those

problems. As all of you well know, there had been legislative proposals to create a national intelligence director (by whatever order of those words) in almost every Congress since 1968—long before the 9-11 Commission recommendation. Nevertheless, as you know, a confluence of events and other factors, including some not insignificant political dynamics, resulted in the passage of that legislation last fall. I hope that the vision you have for that new structure and process will prove to be effective in actual practice.

Clearly DHS needs to *have* intelligence and will to a certain extent develop some intelligence through its own activities, especially in the border and transportation security, to support its operational missions. What is not yet completely clear is what parts of intelligence DHS is expected to obtain for itself and what it receives from others.

Beyond just structure and authority, there are other important considerations. One has to do with what I will call the differences in strategic, operational, and tactical intelligence. Some of us have argued that entities like the Terrorist Threat Integration Center—now becoming the National Counter Terrorism Center (NCTC)—should not be a subordinate of DHS. That entity is in the business of fusing, analyzing, and disseminating intelligence at the “strategic” level for a variety of customers, including DHS, the Department of Justice including the FBI, the Department of State, the Department of Defense, and potentially other federal entities. But that point should not, for a second, be taken to suggest that DHS is not required to have its own robust intelligence capabilities. DHS is a user of NCTC product and develops intelligence information through its own operational entities. It must, therefore, perform fusion, analysis, and dissemination functions that enable effective implementation of its own operational missions and the tactical application of that intelligence at, for example, border points of entry or through distribution to state and local law enforcement or other response agencies.

There is, of course, continuing debate over the extent to which state and local law enforcement should appropriately engage in “intelligence” activities—a significant chorus of voices that suggest that such entities should not be engaged in “spying” on fellow citizens. I believe that no one is suggesting that such activity be forced upon agencies against their will and safeguards exist to preclude that. Nevertheless, many also believe—and I count myself among them—that we have not yet fully taken advantage of the “intelligence”—with a little “i” if you will—that law enforcement agencies obtain every day in the course of ordinary operations that may have some national implications. One need only recall that several of the September 11 hijackers were actually in contact with law enforcement officials for different reasons prior to the attacks. That simple information may not have been enough in itself to alert federal authorities to something amiss but could, when merged with other intelligence or information, identify anomalies for further investigation. The flip side of that discussion is that there are still gaps in the recognition at the federal level of the advantages to be gained from better cooperation with a variety of state and local entities even beyond law enforcement. In passing, I should note that some states and localities have undertaken to establish structures to be more engaged in the process. Notable are the Los Angeles Operational Area Terrorism Early Warning Group (the model of which has now been expanded elsewhere in California), the intelligence and counterterrorism bureaus in the New York City Police Department, and state structures in California, Maryland, Virginia, and elsewhere.

A continuing problem in this area is the determination of what is appropriate and how to share information from the federal level to states and localities and vice versa. There are issues in both the granting of clearances for receiving classified information as well as classification regimes themselves. Entities are struggling to obtain clearances as well as to find ways to pass

information that may not be U.S. national security classified information, in ways alternatively described (though not clearly identified) as “sensitive but unclassified,” “homeland security sensitive,” or “law enforcement sensitive.” It is, in the opinion of some, time to rethink the entire classification process—one perhaps still too embedded in a “Cold War” mentality, to find ways to avoid either the delays in obtaining standard security clearances in the construct of new classification regimes—one that present new and different “tear lines.”

At the risk of lengthening this testimony, I offer discussion on these points and related recommendations contained in the Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (December 2003):

Organizations want more intelligence information about the terrorist threat, but security clearances are lagging.

The RAND survey [conducted for the Panel in 2003] confirmed that State and local organizations are looking to DHS for dissemination of intelligence information and information about the terrorist threat within their jurisdiction or State, in part to help them in conducting their own risk assessments. . .

However, concern exists among State officials that the number of security clearances allocated may still be too few to account for all their needs.

Based on the foregoing, we recommend

- **That the President designate one or more security clearance-granting authorities, which can grant clearances Federal government wide that are recognized by all Federal agencies.** It is incomprehensible that the security clearances of one Federal agency are not recognized by other Federal agencies. . . (B)asic clearances—once granted by a competent authority—should be “portable” to the maximum extent possible.
- **That the President direct the development of a new regime of clearances and classification of intelligence and other information for dissemination to States, localities, and the private sector.** This new regime would remove some of the specific elements that raise the data to a traditional “national security” classification (e.g., sources and methods information) to provide the widest possible distribution to local and State

responders and in a form that conveys meaningful and useful information. Such a process could also prove less expensive and less time-consuming for background investigations and the grant of clearances, as well as more effective in disseminating valuable intelligence.

These and other related intelligence issues are all areas where the Congress will clearly have a continuing role in oversight and authority matters.

Other Management Issues

We also believe that there may also be better ways to rationalize and manage more effectively the personnel, readiness, grantmaking, and research and development programs of DHS. For example, while there are different types of grant programs in DHS, a central body for reviewing the overall grantmaking process across the entire department—one that could ensure that all grant programs are coordinated and implemented in a way that supports national priorities—clearly seems to be warranted. In addition, the promulgation of the National Incident Management System and the National Response Plan are intended, among other things, to provide feedback from federal entities and states and localities that will help to drive future research and development investments. It is not clear that a procedure has been established to accomplish that.

Oversight

The Role of the White House

It is a fact that DHS does not own everything, even at the federal level. The Secretary of Homeland Security has no authority to direct other cabinet officials to do anything nor directly to “command or control” any assets other than those belonging to DHS. Only the President has such authority. With that in mind, the Executive Office of the President—those designated to assist the President in homeland security matters—have important responsibilities to provide continuing strategic guidance and ensure proper coordination of all federal resources through the

development of national strategies and policies. That is not to say that DHS should not a major contributor to the next National Strategy for Homeland Security—we suggest that a new one is needed—nor that DHS should not develop its own internal strategies for the implementation of its designated mission consistent with overall national strategy and policy. But DHS should not be expected to develop the overall national strategy; that is clearly a function for the White House. Fair criticism or not, the Homeland Security Council staff is frequently seen as being more interested in day-to-day homeland security operations than in engaging in the harder task of developing and refining major strategy and policy approaches for the entire nation. In that vein, it is puzzling that the Homeland Security Advisory Committee was moved from the White House to DHS. Certainly the Secretary could benefit from such an advisory body, but would it not be a good idea for the President and his staff to have one that looks objectively and independently at the broader, more strategic national issues—as is the case with other presidential advisory councils and commissions?

Congress as Part of the Problem

Madam Chair and Members, it is perplexing to me, as one who has been engaged in these and similar issues for some years, that the Congress of the United States has not yet fully achieved a coherent logical process for handling these issues. To many of us who are looking at these issues from the outside, it makes no sense that the Department of Homeland Security does not get its *primary* authorization and oversight from a single committee in each House of Congress. No other cabinet agency—one headed by a presidentially-appointed, senate-confirmed secretary—is subjected to the same treatment. It is my opinion that any argument that a single committee cannot be vested with authority to provide that authorization and oversight, because among other reasons that existing committees of jurisdiction have built up essential

experience over the years that cannot somehow be transferred, is fallacious at best. It is patently unfair to saddle this department, especially one that is new and struggling in many areas, with the requirement to report to multiple congressional masters. Common sense dictates otherwise.

Conceptualizing Homeland Security

One area where the Congress or the White House or both should help is in a more clear articulation of the overall *concept* of homeland security. At the time that the term first started to be used in a significant way nationally—right after September 11—it seemed to some to be a convenient title. Yet, it can be argued that there continues to be a lack of national consensus on the scope of homeland security—at the very least a disconnect between consensus and official doctrine.

For example, we have a National Strategy for Homeland Security, promulgated more than two-and-a-half years ago that defines that term only in the context of combating terrorism—specifically “to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.” Although the Homeland Security Act of 2002 did not attempt directly to define the term, it is clear from the subject matter contained in that statute that the Congress has something in mind that would cause that term to be construed more broadly—to include a full range of natural disasters as well as other potential manmade threats, both accidental and intentionally perpetrated.

Terminology, especially definitions and descriptions that go to the very foundations of major national strategy, is important. Is “homeland security” a subset of national security? Some suggest that it is and should be, but we have neither done a good job of saying either that it is or is not nor of naming structures and processes to make that clear. Is homeland defense a

subset of national security or homeland security? This confusion in terminology leads to confusion in the establishment and execution of roles and missions.

Moreover, there is at least the implication that the Department of Homeland Security is responsible—certainly at the federal level—for all of homeland security. There are numerous others players with major roles in this are: the Departments of State, Justice, Defense, and Health and Human Services for starters—and it doesn’t stop there. The existence of DHS has not alleviated the need for intra-agency (within DHS) and federal interagency (between DHS and other federal agencies) as well as intergovernmental coordination. We still need better descriptions and clearer articulation of the roles, missions, and authorities of key stakeholder entities among federal, state, and local governments and with the private sector and the public at large. Unfortunately, we are often slave to history and tradition, culture and bureaucratic boundaries, as we continue to think about shoehorning new missions into old organizational structures, strategies, and processes. Perhaps through specific congressional hearings, or an Executive Branch “summit” that engages all stakeholders, or a combination of the two, an effort should be made to reach a national consensus on what these terms and other terms mean; what are the appropriate roles, missions, and authorities of various entities (including the identification of gaps and overlap in authorities and jurisdiction); and the identification of appropriate measures—legislative, policy or otherwise—that are needed to close gaps and streamline or clarify authorities.

Conclusions

Madam Chair and Members, thank you again for this opportunity. Let me summarize my testimony by suggesting that neither the Congress nor DHS should rush to any judgment about major changes in structure or authority without cautious, deliberate, well-informed,

circumspect—there are other adjectives that apply—debate and consideration. Thorough analysis is required in many areas to inform this policy and decisionmaking process before implementing major change. Clearly, there are some changes that we and others have proposed that rise to the top of the list for consideration in the near term: The creation of a robust policy and planning structure; more holistic approaches in managing risks, the establishment and enforcement, through evaluations and assessments, of a better system of performance metrics. And as noted, both the White House and the Congress have important obligations in providing better strategic guidance and oversight.

Last but by no means least, please continue to consider the fact that the Department of Homeland Security is still relatively new—it has been in existence less than two years. Men and women of good will inside and outside DHS are struggling to make the department work more effectively. DHS has already gone through much turmoil trying to juggle the day-to-day exigencies of threats with the imperatives of merging existing and creating new structures and processes. It will take some time for any major new federal entity—there are instructive historical examples—to operate effectively. It would be well to consider, in that context, the impact of yet more change.

I will, of course, be happy to respond to any questions from the Committee Members.

**"The Department of Homeland Security:
The Way Ahead After A Rocky Start"**

by
Stephen E. Flynn
Jeane J. Kirkpatrick Senior Fellow
for National Security Studies

Chairperson Collins, Senator Lieberman, and distinguished members of the Committee on Homeland Security and Governmental Affairs. I am the Jeane J. Kirkpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations. I am honored to be appearing before you this morning to discuss the vitally important issue of assessing where the U.S. Department of Homeland Security is and where it needs to be to bolster our national capacity to deal with the threat of catastrophic terrorism on U.S. soil.

It is critically important to take stock of where we are for two reasons. First, as with any start-up operation, there is a need to assess whether or not the assumptions that went into creating a new organization have been borne out by its experience after coming online. Since humans are always fallible when it comes to looking ahead into the future, some recalibration inevitably will be required. Second, the stakes associated with fulfilling the Department's mission are enormous. There will almost certainly be attempts to carry out catastrophic terrorist attacks on U.S. soil in the next five years. At the same time, dependable U.S. intelligence capabilities to detect and foil such an attack will not be in place for a decade or more. Since managing the risk of attacks with the potential for mass casualties and profound disruption to our way of life and quality of life is a core governmental responsibility, Americans rightfully expect Congress to diligently exercise its oversight responsibilities on the issues surrounding homeland security.

I admit up front to not being an impartial observer of the Department Homeland Security's growing pains. My feelings today are the same as they were prior to 9/11 when the idea of creating a new department was first contemplated by the U.S. Commission on National Security/21st Century (Hart-Rudman Commission). I remain convinced that successfully bringing our frontline agencies under the management of a single department is indispensable to a credible national effort to protect the U.S. homeland.

There are four compelling reasons why creating the Department of Homeland Security was the right thing to do. First, it is essential to have a cabinet level advocate for bolstering the operational capacity of agencies that play an indispensable role in safeguarding the nation. Throughout the 1990s, the modernization needs of agencies like the U.S. Coast Guard, U.S. Customs Service, and Immigration and Naturalization Service had been largely neglected by their parent departments, the Office of Management and Budget, and congressional appropriators. While their missions continued to grow in size and importance, their means did not. Second, as the work of the 9/11 Commission documented in chilling detail, it is essential to improve the way the federal government collects and distributes sensitive information to frontline agencies about possible terrorist

threats; the connecting-the-dots problem that marred the ability to detect and intercept the 9/11 hijackers. Third, we must enhance the nation's capacity to respond to terrorist attacks. Last it is vital that there be sustained oversight by the White House and Congress of our federal security effort. This is not possible if agencies are sprawled across the government.

Any honest appraisal of the department as it approaches its 2nd anniversary would acknowledge that while there have been significant accomplishments in some areas, we are a very long ways from where we need to be. This is not the fault of the individuals who have selflessly agreed to serve in the department's top leadership posts. No one in the U.S. government has been working harder than the team of people gathered in the cramped office space in DHS headquarters on Nebraska Avenue. But we should not confuse activity with adequate capability. There are three nearly self-evident reasons for limited results. First, we began at a starting line on 9/11 where we were grossly unprepared to manage the terrorist threat at home. Second, there is the very enormity of the task of reducing our national exposure to the threat and consequences of attacks involving weapons of mass destruction and mass disruption. And, third, there are the predictable challenges associated with starting up a new enterprise and managing a large-scale merger and acquisition.

In calibrating expectations of the Department's performance to date, it is helpful to look to the private sector's experience with combining two or more large companies together. Management consultants involved with managing these mergers know that for the first eighteen to twenty-four months, costs generally go up, performance declines, and experienced people leave. It bears little elaboration to posit that the public-sector hurdles for achieving quick results are even greater, particularly when it involves combining twenty two agencies from across the federal government.

While it is appropriate to provide a grace period as the new department works to clear these transition hurdles, with the benefit of hindsight, it is clear that the prospect for a smooth start up has been handicapped by several poor assumptions made at the outset. First, was the unfounded belief that immediate savings and efficiencies could be accrued by standing up the department and identifying and eliminating redundant functions and systems. While those opportunities certainly exist, the first order of business should have been making adequate resources available to overcoming a decade or more of neglect that had left most of these agencies barely able to complete their pre-9/11 non-security missions, never mind their new security mandates.

For instance, the Coast Guard is long overdue in replacing its ancient fleet of cutters and aircraft and modernizing its obsolete shore-based communications system. The stepped-up patrolling requirements attendant with the post-9/11 homeland security and port security mission has only made the need for recapitalization all the more urgent as these aged platforms deteriorate at an accelerated rate. Similarly, now more than ever it is important to complete the long-delayed effort to build the "Automated Commercial Environment" so as to more effectively manage and police the growing volume and velocity of goods that enter the U.S. economy each day. In short, when they stood up the

department, Congress and the administration should have been guided by the conventional wisdom for mergers in the private sector; i.e.; "You have to spend money to save money."

Next, has been a decision to not build within the Office of the Secretary at DHS a cadre of career government senior civil servants. Currently there is just one Senior Executive Service member holding a permanent position in the Office of the Secretary. All the remaining positions are occupied by presidential appointees or personnel "on detail" from one of the agencies belonging to the department. This has translated into rapid turnover of key managers. Indeed, had there been a change in administrations as a result of the 2004 election, the mass exodus of the political appointees could have created nightmarish transition issues for the young department. The heavy reliance on agency detailees to fill the remaining billets in the Office of the Secretary has had the twin consequences of "taxing" these agencies to create the new department by using senior people who draw their salaries from their parent agency and generating the predictable problems associated with relying on managers whose first loyalty is to the bureaucracy they come from and will soon be returning to.

A further challenge has been that the staff support for senior leaders within the department is wholly inadequate for them to effectively execute their demanding responsibilities. For instance, the Deputy Secretary of Homeland Security is supported by a staff of just five individuals. This is unworkable for a position which is equivalent to the Chief Operating Officer of the third biggest federal department in the U.S. government. A consequence of this parsimonious approach to staffing is that few of the challenging policy issues that land in the inbox at the department each day ever get resolved. Further, there is no time or energy left over for the department's leadership to engage in strategic thinking. This is a serious source of frustration for agency managers operating in the field who bump into jurisdictional or doctrinal issues that can only be resolved in Washington. The bottom-line is that managing the transition issues associated with the new department requires a larger staff with longer tenures.

Another unanticipated issue that promises to undermine the ability of the department to meet its mandate is the failure to put in place the training infrastructure that can provide the department's personnel with the new skills they require to carry out their mission. While the average U.S. Navy officer may spend up to forty percent of his or her career receiving training or education, any training provided to the 41,000 employees assigned to the Customs and Border Protection Agency must come at the cost of ongoing operations because there are no training billets built into their personnel system. Reliance on "on-the-job" training is not a sustainable approach to preparing front-line agents to simultaneously enforce immigration, customs, and agriculture laws; to work with sophisticated technologies; and to be able to work in specialized assignments such as being deployed to an overseas port as a part of the "Container Security Initiative." Meeting the department's new mandate require a wholesale reassessment of the legacy personnel systems which were built for simpler jobs in a simpler time.

Another shortfall when the department was created was the failure to provide it with the means to manage the international dimensions of homeland security, especially when involving immigration matters. New security rules invariably have diplomatic, commercial, and trade implications. But the department is not staffed to reach out to other executive departments on an ongoing basis not to handle foreign inquiries. Nor do the State, Treasury, Commerce, Transportation, Agriculture, and Health and Human Services departments, along with the U.S. Trade Representative, have senior people assigned to focus on the dimensions of homeland security that involve their responsibilities. Inevitably, clashes among competing U.S. interests that could have been anticipated and minimized by good upfront coordination turn into bureaucratic brush fires that consume the very finite time and energy of top-officials who must endeavor to extinguish them.

One particularly gray area that the department must sort out is how to interact with the Department of Defense. The Pentagon has been keen to maintain its autonomy by assigning itself the mission of “homeland defense,” which it defines as involving terrorist attacks that emanate only from outside the United States. Relying on this definition, defense planners have essentially found a way to carve out a niche where the armed forces patrol air space and the high seas, and prepare for catastrophic terrorists attacks when they happen, but largely in isolation of the planning process within the Department of Homeland Security. The artificial line drawn between homeland defense and homeland security needs to reexamined with an eye towards expanding the operational support role the Department of Defense will play in carrying out the Department of Homeland Security’s mission.

Finally, the department needs a far more robust framework for engaging with the private sector on the issues associated with critical infrastructure protection. As a stepping off point, the administration must acknowledge that its assumption that the private sector would invest in meaningful security for the 85 percent of the nation’s critical infrastructure that it owns—and upon which our way of life and quality of life depends—has not been borne out. We now have three years of survey data which confirms that the level of spending on prudent security measures is modest at best. The explanation for this is that it turns out there is not a market case for the private sector to secure itself. Without clearly defined security requirements, private companies are not investing in comprehensive security measures to protect infrastructure they depend on because their executives worry that such investments will place them at a competitive disadvantage. They also worry that if they make an independent decision about “how much security is enough” which is not endorsed by the public sector, they will expose themselves to liability issues should their security efforts be found wanting in the aftermath of an attack. A consequence of limited federal leadership in this area has been inertia. The Department of Homeland Security must move beyond identifying “best practices” and instead identify meaningful incentives and mechanisms for the private sector to become a real partner in reducing the many soft targets that remain an open invitation for terrorist organizations to do their worst of U.S. soil.

At the end of day, the measure of success of the Department of Homeland Security is not whether good people made good faith efforts to address many of the security shortcomings exposed by the 9/11 attacks. The judgment of history will be whether those changes were made with the sense of urgency that the threat warranted. I worry that unless we treat the homeland security agenda with the same intensity of effort we are marshalling for the war on terrorism abroad, the U.S. government will not pass that test. Sadly, the consequence will be not just the preventable loss of life and property. The fallout also is likely to extend to a severe loss of public confidence in the federal government when it is determined that not enough was done to meet its core responsibility of providing for the safety and security of the American people. In short, the stakes associated with the important work of this Committee could not be higher.

Thank you Madam Chairperson for this opportunity to testify before you on this vitally important issue. I look forward to responding to your questions.

Stephen Flynn is the author of *America the Vulnerable*, published by HarperCollins in July 2004. He is the inaugural occupant of the Jeane J. Kirkpatrick Chair in National Security Studies at the Council on Foreign Relations. Dr. Flynn served as Director and principal author for the task force report *“America: Still Unprepared—Still in Danger,”* co-chaired by former Senators Gary Hart and Warren Rudman. He spent twenty years as a commissioned officer in the U.S. Coast Guard including two commands at sea, served in the White House Military Office during the George H.W. Bush administration, and was director for Global Issue on the National Security Council staff during the Clinton administration. He holds a Ph.D. and M.A.L.D. from the Fletcher School of Law and Diplomacy and a B.S. from the U.S. Coast Guard Academy.

STATEMENT OF
RICHARD A. FALKENRATH
VISITING FELLOW
THE BROOKINGS INSTITUTION
BEFORE THE
UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

January 26, 2005

Introduction

Good morning, Madam Chairman, Senator Lieberman, and Members of the Committee.

I am grateful for the opportunity to be here today to provide my views on the present and future challenges facing the Department of Homeland Security (DHS). I would also like to express my gratitude to the Members of the Committee on Homeland Security and Governmental Affairs. You have played a central role in developing two vital pieces of post-9/11 legislation: the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004. These are historic accomplishments.

Assessment of DHS Management

My direct experience with the DHS management extends only to mid-May 2004, when I resigned my position as Deputy Homeland Security Advisor to the President. Nonetheless, I will offer a few general comments on this subject.

Managing the start-up of the Department of Homeland Security is surely one of greatest managerial challenges any Cabinet officer has ever had to face. The scale and

complexity of the task can hardly be underestimated; the time frame for action was tight and unforgiving; the daily operational and policy demands were relentless; the interagency environment could be treacherous; the external constituencies, perpetually discontented. With circumstances such as these as backdrop, no Cabinet officer will ever succeed at all tasks, all the time. The real question, however, is not whether there are some tasks that a Cabinet officer and his lieutenants have not performed adequately - of course there are and always will be. The real question is whether a Cabinet officer has accomplished the highest priorities objectives assigned to him or her by the President or the Congress. Measured by this yardstick, I believe that the Secretary Ridge and his subordinates have exceeded all reasonable expectations of their performance and are more deserving of commendation than complaint.

Even leaving aside the substantive accomplishments of the Department of Homeland Security during its first two years of existence, the strictly managerial accomplishments of the Department are considerable. On March 1, 2003, 22 agencies transferred to DHS, each with distinct human resource policies and systems; the Department currently utilizes just seven human resource servicing offices. The Department started with 19 financial management service providers; it now utilizes eight. The Department started with seven different payroll providers for the Department; it now has two. The Department started with 27 Consolidated Bank Card Programs; it now has three. These statistics are testament to the real integration that occurred within the Department in its first two years of existence, but they are themselves merely a few items contained within the Department's comprehensive strategic plan - a document that was worked out

in cooperation with the Homeland Security Council and that contains over 900 specific goals and milestones with associated timelines.

I have reviewed the December 2004 report of the DHS Inspector General, "Major Management Challenges Facing the Department of Homeland Security." I do not doubt that some of the specific criticisms levied against the Department are true, but I find the report seriously lacking in that it offers no comprehensive net assessment of the Department's overall managerial performance or its strategic plan. Indeed, the report failed to persuade me that the managerial performance is any way significantly worse than that of any other major federal department or agency - none of whom have had to cope with the unique challenges associated with the largest government reorganization in 50 years.

In my experience, every major federal department and agency has management challenges and deficiencies of one kind or another. The FBI, for example, has had trouble with its computer modernization, laboratory, and fingerprint system accuracy; the FDA has had trouble with its drug approvals; the Air Force has had trouble with certain large aircraft procurements; the national laboratories have had trouble with their security procedures; the Department of Interior has had trouble with the American Indian trust fund; the IRS has had trouble with its computer modernization; NASA has had trouble with its flight safety program; etc. No federal department or agency is immune to management failure. Indeed, I suspect the management record of even the

best managed government agencies is worse than that of mediocre for-profit companies.

The central fact of federal government management today is that the unilateral managerial authority of federal agency heads is a fraction of that enjoyed by their private-sector counterparts. The Department must operate within the confines of its authorizing statutes; spend money only according to the terms of its appropriations bills; hire only those senior officials who have been selected by the President and confirmed by the Senate; and announce new policies and regulations only after they have gone through laborious interagency vetting and clearance. Compared to most other Cabinet offices, the Secretary of Homeland Security has a few additional managerial flexibilities but certainly not enough to make his flexibility comparable to that which is commonplace in the private sector. These considerations should be taken into account before one passes judgment on a government manager's performance.

Congressional Oversight of DHS

I commend the action taken by the House and Senate Appropriations Committees at the beginning of the 108th Congress - namely, the creation of a separate Appropriations Subcommittee with sole responsibility for authoring the annual DHS appropriations bills. These two subcommittees performed superbly in their first two years of existence, writing two strong appropriations bills that were delivered to the President's desk on time and with very few "earmarks." These two subcommittees have become genuine

partners in the evolution of the Department of Homeland Security, and the Administration understands the need to be highly responsive to their requests for information and consultation.

The role of the authorizing committees with jurisdiction over some portion of the Department of Homeland Security has been completely different. The 9/11 Commission termed Congressional oversight in this area "dysfunctional," concluding:

Congress needs to establish for the Department of Homeland Security the kind of clear authority and responsibility that exist to enable the Justice Department to deal with crime and the Defense Department to deal with threats to national security. Through not more than one authorizing committee and one appropriating subcommittee in each house, Congress should be able to ask the secretary of homeland security whether he or she has the resources to provide reasonable security against major terrorist acts within the United States and to hold the secretary accountable for the department's performance.

I agree. The demands upon various officers within the Department of Homeland Security to testify before various authorizing committees of both Chambers is incommensurate with the ability of these of any of these committees to pass legislation that will assist the Department fulfill its responsibilities or accomplish its mission. Department of Homeland Security officials face a far greater burden of testifying before Congressional committees than do their counterparts in other federal departments

and agencies. Members who serve on these overlapping oversight committees should not be surprised if the Department is at times less than fully responsive to their requests for information or consultation.

Many Members of Congress have expressed concern about that internal management of the Department. I believe that the quality of this management will improve if senior Departmental leadership is allowed to spend more time on internal management tasks. Reducing the time-burden of Congressional testimony would be a step in the right direction. An even more important step, however, would be to permit the Department to develop a serious and comprehensive oversight arrangement with a single authorizing committee.

Internal DHS Organization

A number of outside experts have recently begun to circulate proposals for modifying the internal organization of the Department. There is nothing sacrosanct in the Department's present internal structure but I do not believe that a statutorily driven redesign of the Department at this time is either warranted or wise, for four reasons.

- First, the second Secretary of Homeland Security is about to be appointed. He deserves the opportunity to familiarize himself with the Department and its mission, to form his own opinion about what organizational changes beneath him

will improve his ability to fulfill his responsibilities, and to make appropriate recommendations to the President for consideration as legislative proposals.

- Second, the Department of Homeland Security is presently at a stage of organizational development in which it must follow through and complete the original reorganization concept for the Department. It is too early to draw a firm conclusion that this original concept was grossly misguided, and too early to give up on its implementation.
- Third, the Secretary of Homeland Security already has certain limited reorganization authorities. If there is a near-term need to create a new office or appoint a new Assistant Secretary, for instance, the Administration can do so under existing statutes.
- Fourth, if our recent experience with government reorganization has taught us anything, it has taught that reorganization is an immensely distracting endeavor that imposes a significant near-term performance penalty on the entity being reorganized. This penalty is worth incurring only if the long-term benefits of the reorganization are truly compelling. I am not persuaded that this is the case in any reorganization proposals being proposed by outside experts at this time.

One step that Congress could usefully take that this time would be to enhance the Secretary's unilateral reorganization authority in such a way that will allow him to make necessary organizational refinements, once he determines what they are, quickly and efficiently. Specifically, I would recommend that the Congress consider:

- Amending the Department's personnel authorization (Section 103 of the Homeland Security Act) to eliminate the specific titles of the Under Secretaries and instead permit the appointment of up to seven Under Secretaries with titles to be determined by the President, subject to the advice and consent of the Senate.
- Amending the Secretary's reorganization authority (Section 872 of the Homeland Security Act) to permit the abolition of entities, programs, and functions required by the Act, and to make this authority "notwithstanding any other provision of law."
- Directing the Secretary to coalesce the regional boundaries of various units of the Department into a single regional structure, and to streamline the reporting relationship of all Department staff as he sees fit.
- Enlarging dramatically the modest reprogramming authority contained within the Department's 2004 and 2005 appropriations bills.

- Authorizing a flexible, substantial working capital fund more in line with other major Cabinet agencies, such that of the Department of Justice.

I would be pleased to comment on any of the particular proposals for reorganizing the Department being advanced by outside experts later in the hearing.

Security Priorities for DHS, 2005-2006

The efficient management of the Department of Homeland Security is an important objective, but it is not the Department's foremost priority. Looking ahead, the most important challenge for the Department of Homeland Security is to weave ever greater levels of security into the fabric of American society. This is the substance of the Secretary of Homeland Security's job, and is the essence of his political contract with the President, the American people, and their elected representatives. Prior to the creation of the Department of Homeland Security, there was no Cabinet office with this job description. Today there is, and this alone was sufficient reason to establish the Department.

I will not offer a description of the Administration's or the Department's past and on-going accomplishments in the field of homeland security. Instead, I will provide a personal assessment of the highest priority work that remains to be. I will focus on five

areas that fall largely, though not exclusively, within the domain of the Department of Homeland Security.

1. Credentials and Identification Standards

The federal government should establish a voluntary national standard for secure identification. This standard should meet the requirement set by the President for federal government identification documents in Homeland Security Presidential Directive 12, namely: "identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application." After the standard has been promulgated through normal procedures, the provision of identification meeting this standard should be required at all federally controlled portals that are important to security.

This standard should incorporate and supersede all other federal identification programs. Once the standard has been promulgated, the particulars of the identification program will become inconsequential.

It is clear that any decent identification standard will include a strong biometric identifier that associates the person bearing the identification with the person who received it, a

so-called "one-to-one" match. In addition, however, the federal government also has an invaluable counterterrorism opportunity to conduct "one-to-many" screening against a biometric reference database of known and suspected terrorists. Since the only such reference database in existence is fingerprint-based, it is clear an identification standard that incorporates ten fingerprints will yield the best security benefits.

2. Expanded Screening against the Alphanumeric and Biometric Terrorist Watchlists

The United States and its allies spend billions of dollars each year, and risk countless lives, to acquire terrorist identifying information. This information is now consolidated into two primary systems: alphanumeric data is maintained in the terrorist identities and screening database managed by the National Counterterrorism Center and the Terrorist Screening Center; while biometric data (fingerprints) is maintained by the FBI's Integrated Automated Fingerprint Identification System. These terrorist reference databases require continual improvement but they are the best of their kind in the world.

The policy of the United States should be to apply this terrorist-identifying information at every available opportunity. Put differently, the United States should develop and deploy name-based and fingerprint-based screening systems that will create opportunities to identify, apprehend or exclude known or suspected terrorists before they carry out their attacks. These systems are already in place at visa-application stations, most points of entry (through the U.S. VISIT system), and in the National Instant Criminal Background Check System, but there are many more public and

private-sector screening opportunities that have not yet been exploited. The Department of Homeland Security should lead the expansion of terrorist screening at home. In addition, the United States should encourage its international partners to deploy compatible screening systems and should promote real-time, cross-border reciprocal querying of terrorist watchlists. The Department of Homeland Security should assist the Department of State in promoting such screening abroad.

3. Hazardous Chemical Security and Protection

The essence of Al Qaeda's strategy for causing catastrophic harm to America on September 11 was to strike an inherently dangerous, poorly secured system in our midst. Due to the passage of the Aviation and Transportation Security Act and the work of the Transportation Security Administration, passenger aircraft are no longer poorly secured and hence no longer fall into this target category. It stands to reason that, in the aftermath of September 11, our terrorist enemies are surveying American society to locate other inherently dangerous, poorly secured systems that they could strike with catastrophic secondary effects. Fortunately, the number of such severe vulnerabilities is finite. One, however, stands out at acutely vulnerability and almost uniquely dangerous: toxic-by-inhalation industrial chemicals. These poorly secured chemicals, which in some cases are identical to the chemical weapons used in World War I, are routinely present vast, multi-ton quantities adjacent to or in the midst of many dense population centers. Toxic-by-inhalation industrial chemicals present a mass-casualty

terrorist potential rivaled only by improvised nuclear devices, certain acts of bioterrorism, and the collapse of large, occupied buildings.

To date, the federal government has made no material reduction in the inherent vulnerability of hazardous chemical targets inside the Untied States. Doing so should be the highest critical infrastructure protection priority for the Department of Homeland Security in the next two years. The executive branch currently as sufficient regulatory authority to require virtually any security enhancement for chemicals as they are being transported, so executive action is required but new legislation is not. With respect to chemical facilities, the executive branch currently lacks the authority to mandate and enforce security enhancements. The President twice called on the 108th Congress to pass such legislation. The 109th Congress should heed his call.

4. Ground Transportation System Security

Under the authorities granted by the Aviation and Transportation Security Act and the Maritime Transportation Security Act, and through the work of the Transportation Security Administration and the U.S. Coast Guard, the federal government has made great strides in improving the security of air and sea transportation systems. No real progress, however, has been made in the area of ground transportation security. The operational challenge of securing these ground transportation sectors far exceeds that of securing airports, but the Department of Homeland Security should lead an effort to systematically reduce the vulnerability of U.S. rail, mass-transit, and trucking

transportation systems. There is no "silver bullet" in this domain, but an appropriate security system is certain to include some combination of access control, telematic tracking, geo-fencing, and sensor-based domain awareness. No new statutory authority is required for such an effort given the robust regulatory authorities contained within the Aviation and Transportation Security Act.

5. Terrorism Insurance

Prior to September 11, 2001, most commercial insurance policies covered terrorist losses. This gave private companies as certain market-based incentive to secure their buildings against terrorism, spread the economic risk associated with terrorist across the economy, reduced the federal payout after the attack.

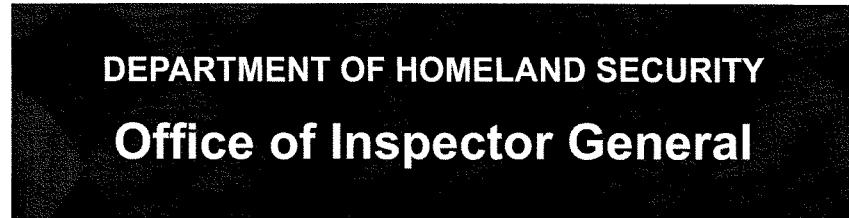
After the catastrophic losses of September 11, 2001, primary insurers began to drop terrorism coverage from their commercial policies. The federal government sought to slow this trend by backstopping the reinsurance industry under the authority granted in the Terrorism Risk Insurance Act of 2002. This act is scheduled to sunset in 2005 and has, in any case, failed to accomplish its most important objective - namely, to promote the sharing of terrorist risk and the implementation of security countermeasures at commercial facilities nationwide.

Congress should reauthorize the Terrorist Risk Insurance Act but should go a step further in order to make the program more valuable from a security point of view.

Congress should mandate that terrorism coverage be included in all commercial insurance policies, and should transfer responsibility for the program from the Department of Treasury to the Department of Homeland Security. Congress should also charge DHS with developing, in cooperation with the insurance industry, standards for private-property protective measures that would lead to premium reductions.

Conclusion

Madam Chairman, I would like to thank you and the Members of your Committee for your continuing service to the country. Thank you again for the opportunity to appear the Committee today. I am happy to answer any questions you may have.



**MAJOR MANAGEMENT CHALLENGES FACING
THE DEPARTMENT OF HOMELAND SECURITY**



Office of Audits
OIG-05-06 December 2004

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528



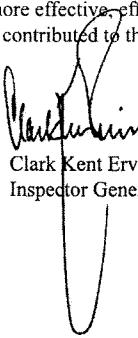
**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, investigative, and special reports prepared by the OIG as part of its DHS oversight responsibility to identify and prevent fraud, waste, abuse, and mismanagement.

This report presents OIG's assessment of "major management challenges" facing DHS. It is based on issued reports, interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents. These challenges are a major factor in setting OIG's priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the Reports Consolidation Act of 2000, OIG updates its assessment of management challenges annually for inclusion in DHS' Performance and Accountability Report.

It is my hope that this report will result in more effective, efficient, and economical operations. I express my appreciation to all of those who contributed to the preparation of this report.


Clark Kent Ervin

Inspector General

Office of Inspector General

**U.S. Department of
Homeland Security
Washington, DC 20528**



November 1, 2004

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

During its first 20 months of existence, the Department of Homeland Security (DHS) worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the critical, core mission of protecting the country against another terrorist attack, has presented many challenges to the department's managers and employees. While DHS has made progress, it still has much to do to establish a cohesive, efficient, and effective organization.

The Office of Inspector General (OIG) identified "major management challenges" facing the department, as discussed below. These challenges are a major factor in setting DHS OIG priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the Reports Consolidation Act of 2000, the OIG will update its assessment of management challenges annually.

CONSOLIDATING THE DEPARTMENT'S COMPONENTS

Integrating its many separate components into a single, effective, efficient, and economical department remains one of DHS' biggest challenges. DHS has made notable progress in this area. For example, DHS established an Operational Integration Staff to assist departmental leadership with the integration of certain DHS missions, operational activities, and programs at the headquarters level and throughout the DHS regional structure. However, much remains to be done and structural and resource problems continue to inhibit progress in certain support functions.

For example, while the department is trying to create integrated and streamlined support service functions, most of the critical support personnel are distributed throughout the components and are not directly accountable to the functional Line of Business (LOB) Chiefs. On the other hand, the Chief Procurement Officer (CPO), Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Human Capital Officer (CHCO), and Chief

of Administrative Services (CAS) have been directed to lead the development of management and integration efforts for their respective function, and have been given the responsibility of optimizing a department-wide support structure that eliminates redundant efforts.

In August 2004, the Secretary and Deputy Secretary directed the DHS LOB Chiefs to design and implement systems that will optimize their functions across the entire department and develop Management Directives to guide the department's management of that business function. The Directives are to build on a concept of "dual accountability" where both the operational leadership and the LOB chiefs are responsible for the successful preparation of Directives that will govern the work and the implementation effort that follows their preparation. The Deputy Secretary described the concept as a "robust dotted line" relationship of agency or component functional heads to the LOB chiefs for both daily work and annual evaluation. Final Management Directives are expected to provide direction for both process and resource management. The Secretary and Deputy Secretary called for these documents to be issued in mid-September 2004 in order to institutionalize the arrangements before FY 2005. As of October 15, while the department had not released any final Management Directives, the department's Management Council and appropriate departmental councils (i.e., CIO Council, etc.) had approved each of the Management Directives related to each LOB. In addition, Council charters have been signed for each LOB that signify concurrence among the organizational elements (OEs) of the department and establishes a formal governance and advisory board structure to ensure that the objectives and intent of the Directives are executed.

OIG will be monitoring and evaluating these efforts closely.

CONTRACT MANAGEMENT

DHS obligated about \$6.8 billion procuring goods and services during FY 2003. In addition to the challenge of integrating the procurement functions of its component organizations, DHS must provide contract management to the OEs that came into the agency without the accompanying procurement staff. These components include the Science and Technology (S&T) Directorate, the Information Analysis and Infrastructure Protection (IAIP) Directorate, the Office of State and Local Government Coordination and Preparedness, U.S. VISIT, and other departmental operations. DHS formed the Office of Procurement Operations (OPO) to provide procurement support for these components, but the office has insufficient staff to manage over \$2.5 billion in procurements. DHS has contracted with other federal agencies to provide the contract management support needed while it addresses the resource issues in OPO. However, providing consistent contract management throughout DHS remains a formidable challenge. The OPO has developed and negotiated with its customer organizations a staffing plan for OPO that would bring OPO's staffing level to 127 by the end of FY 2005. The cost of these positions would be reimbursed by customer organizations through the Working Capital Fund.

DHS' efforts to provide a sufficiently detailed and accurate listing of procurement information proved difficult and were hampered by existing federal systems. While DHS has migrated all of its procurements under the umbrella of one comprehensive reporting system, the department still lacks sufficiently detailed and validated data for FY 2003 and FY 2004 to manage the procurement universe and ensure accurate and consistent reporting.

The DHS OEs also face continuing challenges in contract management, but have made some progress. For example, the Transportation Security Administration (TSA) relies extensively on contractors to accomplish its mission, but during its first year of operation, provided little contract oversight. As a result, the cost of some of those initial contracts ballooned. In 2004, however, TSA began implementing policies and procedures to provide improved procurement planning, contract structure, and contract oversight.

Several DHS OEs have large, complex, high-cost procurement programs under way that need to be closely managed. For example, CBP's Automated Commercial Environment (ACE) project will cost \$5 billion, and the Coast Guard's Deepwater Capability Replacement Project will cost \$17 billion and will take two to three decades to complete. Further, the department recently awarded a \$10 billion contract for the development of a system to support the United States Visitor and Immigrant Status Indication Technology (US-VISIT) program for tracking and controlling the entry and exit of all aliens entering and leaving the country through air, land, and sea ports of entry. According to departmental officials, this program is on track to be implemented fully within the next ten years. Also, TSA's managed information technology services contract will cost over \$1 billion. DHS OIG will be reviewing these major procurements on an ongoing basis.

GRANTS MANAGEMENT

DHS manages a variety of grant programs, totaling approximately \$10 billion in obligations for 2003, which provide money for disaster preparedness, prevention, response, and recovery. Significant shortcomings have been identified in many of these programs in the past, including the potential for overlap and duplicate funding. In an effort to achieve better coordination, the Office for Domestic Preparedness and Office of State and Local Coordination were consolidated into the Office of State and Local Government Coordination and Preparedness (SLGCP). That office is responsible for 25 preparedness grant programs, including first responder grants.

However, much work remains to be done. In March 2004, the OIG issued *An Audit of Distributing and Spending "First Responder" Grant Funds, OIG-04-15*. The report identified problems at the state and local level that were causing grant fund distribution and spending to be slow. The problems included too many large grant programs that had to be processed in too short a time with inadequate state and local staffing; a lack of federal guidance on preparedness standards; complex and time consuming state and local planning processes; and burdensome state and local procurement and grant approval processes. The department is taking action to minimize state and local governments' problems and provide

more assistance. For example, DHS developed a grants management technical assistance program for state and local grantees.

On March 15, 2004, Secretary Ridge formed the Task Force on State and Local Homeland Security Funding to examine why federal funds were not reaching local governments and first responders in a timely fashion. In June 2004, the Task Force issued its report, and DHS officials said that it is incorporating the recommended actions in the Task Force report to produce measurable progress in grant fund distribution and spending.

The OIG is currently conducting audits of individual states' management of first responder grants and analyzing the effectiveness of DHS' system for collecting data on state and local governments' risk, vulnerability, and needs assessments. The OIG will continue its audits of the department's disaster relief programs, and, in FY 2005, will conduct audits of state and local governments' use of first responder grant funds.

In assessing DHS grant management operations, the advice of the 9/11 Commission is pertinent. It recommended, "[F]ederal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support."¹ In the OIG's recent draft report on the DHS Port Security Grant program, the OIG reported that DHS grant making for this sector of national infrastructure was not well coordinated with the IAIP Office of Infrastructure Protection, did not account for infrastructure protection priorities in the application review process, and resulted in funding of projects with low scores in the review process. Also, the DHS does not have a strong grant evaluation process in place by which to address post-award administration issues, including measuring progress in accomplishing DHS' grant objectives.

Department officials note that SLGCP, the United States Coast Guard, the Department of Transportation's Maritime Administration (MARAD), and TSA are partners in the Request for Application development as well as the evaluation panels for the Port Security Grant Program. As the lead agency for port security, the United States Coast Guard has been working with IAIP on port-wide criticality assessments. The Port Security Grant Program requires applicants to have completed a security vulnerability assessment as required in the Maritime Transportation Security Act (MTSA). The United States Coast Guard has defined the criteria for the structure of the required vulnerability/risk assessments under MTSA. Department officials said that in FY 2005, SLGCP will involve IAIP's Office of Infrastructure Protection appropriately in the Port Security Grant Program.

Department officials also said that staffing is inadequate to supporting the administration of the Port Security Grant Program's post-award phase. Staff developed a report to be submitted by the grantee at the end of the project period. This data will provide broad statistics demonstrating how the grant award funding has reduced the grantees' risk as identified by their security vulnerability assessment. Department officials said that in FY 2005, SLGCP plans to increase staff to allow for site visits and improved oversight of grant-funded projects.

¹ Final Report of the National Commission on Terrorist Attacks upon the United States, page 396 (2004).

FINANCIAL MANAGEMENT

Integration and Reporting

In March 2004, the department issued its first *Performance and Accountability Report* (PAR), containing its first set of published financial statements. The department received a qualified opinion on its balance sheet as of September 30, 2003, and the statement of custodial activity for the seven months then ended. This was a significant accomplishment for a large and complex department that was just starting-up. This effort produced a baseline for improvement with identification of 14 reportable conditions, seven of which were considered to be material weaknesses.²

The material weaknesses consisted of control weaknesses in the following areas:

- A. Financial Management and Personnel
- B. Financial Reporting
- C. Financial Systems Functionality and Technology
- D. Property, Plant, and Equipment
- E. Operating Materials and Supplies
- F. Actuarial Liabilities
- G. Transfers of Funds, Assets, and Liabilities to DHS

The other reportable conditions consisted of control weaknesses in these areas:

- H. Drawback Claims on Duties, Taxes, and Fees
- I. Import Entry In-bond
- J. Acceptance and Adjudication of Immigration and Naturalization Applications
- K. Fund Balance with Treasury
- L. Intra-governmental Balances
- M. Strategic National Stockpile
- N. Accounts Payable and Undelivered Orders

The department had very little time to focus on correcting the above deficiencies before the start of the FY 2004 audit. Therefore, most material weaknesses and reportable conditions will carry forward into the FY 2005 audit report. The material weakness associated with transfers of funds, assets, and liabilities to DHS was specific to DHS' first reporting period and will not be carried forward. In August 2004, the Strategic National Stockpile was transferred to the Department of Health and Human Services and is no longer the

² Specifically, the American Institute of Certified Public Accountants define reportable conditions as "matters coming to the auditors' attention relating to significant deficiencies in the design or operation of internal controls that, in the auditors' judgment, could adversely affect the department's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements." Material weaknesses are defined as "reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions."

responsibility of DHS. Finally, the Secret Service resolved its material weakness regarding actuarial liabilities.

In FY 2004, the department faced reporting problems stemming from the reorganization of the former Immigration and Naturalization Service (INS) and the U.S. Customs Service into three new bureaus -- Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS), referred to as the "tri-bureaus" -- and the consolidation of accounting services for many small programs from outside of DHS into ICE. However, the department and ICE did not prepare a thorough, well-designed plan to guide the transition of accounting responsibilities within ICE. ICE fell seriously behind in the performance of basic accounting functions, such as account reconciliations and analysis of abnormal balances. The pervasiveness of errors in ICE's accounts will prevent the auditors from completing their work at ICE for the FY 2004 DHS financial statement audit.

At Coast Guard, the auditors will not be able to complete audit work this year on all accounts because of difficulties encountered. These difficulties will result in additional material weaknesses that will be reported in the upcoming FY 2004 audit report.

The department also faces a structural problem in its financial management organization. The bureaus control most of DHS' accounting resources, but the DHS Chief Financial Officer (CFO) has responsibility for DHS' consolidated financial reporting, which is dependent on those resources. Although coordination mechanisms are in place, monitoring controls at the DHS CFO's level are insufficient to ensure the accuracy of consolidated financial information. The seriousness of the material weaknesses and reportable conditions at DHS demands strong DHS CFO oversight and controls.

In October 2004, the President signed the Department of Homeland Security Financial Accountability Act (Act), a law that will significantly challenge the department's managers. The Act will require the department to make an assertion as to the effectiveness of its internal control structure beginning in FY 2005. In addition, proposed changes to OMB's Circular A-123 would require substantial agency resources and efforts to comply with the Circular's internal control documentation and reporting requirements. To complete this task, the department's financial managers will need to identify and document existing processes related to financial reporting, then perform their own testing of the design and effectiveness of internal control mechanisms and procedures. This requirement, similar to that levied on publicly traded companies under the Sarbanes-Oxley Act, goes far beyond any previous management review of internal controls over financial reporting performed by DHS. DHS will have to ensure that it complies with all standards of the Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* in order to achieve a clean audit opinion on internal control over financial reporting in FY 2006.

Revenue Collection

Annually, CBP collects more than \$22 billion in duties, excise taxes, fines, penalties, and other revenue. CBP has had an active program to monitor trade compliance, but in the face

of critical homeland security responsibilities, counter-terrorism activities have begun to claim a higher share of border resources. CBP faces a challenge in protecting trade revenue and enforcing trade laws at a time when the terrorist threat demands much more from CBP's border resources.

CBP is responsible for collecting user fees from air passengers arriving in the United States. The fees are designed to offset the costs of inspection services provided by CBP, which now includes the former INS and the Animal and Plant Health Inspection Service (APHIS) inspection processes. Between FYs 1998 and 2002, the former U. S. Customs Service collected \$1.1 billion from the airlines. Now that CBP's inspection workforce has expanded to include the former INS and APHIS inspection services, it is important that CBP ensure that revenues collected are accounted for and are adequate to cover the costs of services provided. In addition, the TSA is required to impose a fee on airline passengers. This fee is designed to offset the costs of providing civil aviation security services provided by screening personnel, Federal Air Marshals, and equipment. The OIG and GAO are currently auditing the collection of airline passenger fees.

USCIS generates more than \$1 billion in revenues through collection of immigration and naturalization application fees from non-citizens seeking entry into the United States. In fulfilling its mission, USCIS processes millions of actions and requests that are documented in paper files. The systems that track these applications are not integrated, and many are *ad hoc*. Deferred revenue is a financial measure of pending applications and is material to DHS' financial statements. The challenge for USCIS is to move from paper based and non-integrated processes to an integrated case management system.

HUMAN CAPITAL MANAGEMENT

The Homeland Security Act gave DHS special authorization to design a human capital management system that fits its unique missions. On April 1, 2003, the department announced that it would assemble a team of diverse employees from across the department and representatives from OPM and major unions to design a new human capital management system for the department's approximately 180,000 employees. This team developed a range of options for pay and classification, performance management, labor relations, discipline, and employee appeals that were presented to the Secretary and the Director of OPM. The decisions of the Secretary and the Director were published as proposed regulations and public comments were received. DHS received over 3,500 comments from employees, DHS employee unions, the general public, and members of Congress during the public comment period. DHS spent four weeks with major DHS employee labor union representatives in congressionally mandated "meet-and-confer" sessions and then extended that process for an additional two weeks. Secretary Ridge and Director James personally met with the presidents of the two largest DHS employee labor unions in early September 2004. DHS continues to carefully review and consider the issues raised in those forums. Once that review is completed, department officials say that it will move forward with a new human resource management system that will support the mission of the Department of Homeland Security while recognizing the rights of its employees. According to the department, these

new regulations will dramatically affect not only DHS employees, but also, at least potentially, the entire civilian workforce, as the DHS system will likely be considered a model for civilian personnel programs government-wide. In June 2004, the department awarded a contract for services related to the development and implementation of a new human resource system, MAXHR.

An additional serious problem involves the length of time necessary to complete the security clearance process, even for federal employees from other agencies who hold clearances when they enter DHS. At the same time, several OIG reviews have noted flaws in the background investigations of new employees, notably the reviews of TSA's screeners and the Federal Air Marshals Service. The OIG does not advocate a reduction of diligence in the personnel security process, but notes that the delays are long and have adversely affected DHS' operations.

INTEGRATION OF INFORMATION SYSTEMS

Creating a single infrastructure for effective communications and information exchange remains a major management challenge for DHS. To meet this challenge, the chief information officer (CIO) has efforts under way to determine the strategies and technologies needed to connect the local, metropolitan, and wide area networks of the department's legacy agencies. Specifically, DHS enhanced the ICE's telecommunications "backbone" to create the department-wide network, establishing data communications for the establishment of the department's initial capability. Subsequently, a new concept has been developed and an initiative is under way to create the department-wide network that will establish common policies and technical standards for data communications among all organizational components. Further, the CIO is working with line managers to complete a second version of enterprise architecture to guide management of information and technology in the department. The CIO released the first version of the architecture in September 2003, and is now working to make its transition strategy more detailed and easier to implement and align with several of DHS' large information technology (IT) projects. Additionally, DHS has established the "eMerge" program,³ scheduled for implementation by September 2006, to integrate the redundant and nonintegrated systems used to support administrative activities such as accounting, acquisition, budgeting, and procurement.

However, as the OIG reported in July 2004, the DHS CIO is not well positioned to meet the department's IT objectives. Despite federal laws and requirements, the CIO is not a member of the senior management team with authority to strategically manage department-wide technology assets and programs. No formal reporting relationship is in place between the DHS CIO and the CIOs of major component organizations, which hinders department-wide support for his central IT direction. Further, the CIO has limited staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support departmental units. These deficiencies in the IT organizational structure are exemplified by the CIO's lack of oversight and control of all DHS' IT investment decision-

³ Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency (eMerge²).

making and a reliance instead on cooperation and coordination within DHS' CIO Council⁴ to accomplish department-wide IT integration and consolidation objectives. The department would benefit from following the successful examples of other federal agencies in positioning their CIOs with the authority and influence needed to guide executive decisions on department-wide IT investments and strategies.

SECURITY OF INFORMATION TECHNOLOGY INFRASTRUCTURE

The security of IT infrastructure is a major management challenge. As required by the Federal Information Security Management Act (FISMA), the CIO must develop and implement a department-wide information security program that ensures the effectiveness of security controls over information resources that address the risks and vulnerabilities facing DHS' IT systems.

As DHS OIG reported in September 2004, based upon its annual FISMA evaluation, DHS has made significant progress over the last year in developing, managing, and implementing its information security program at the departmental level. The Chief Information Security Officer (CISO) updated many of its IT security policies and procedures and together, these policies and procedures, if fully implemented by the components, should provide DHS with an effective information security program that complies with FISMA requirements.

Even though DHS has made several improvements in its information security program, the OEs have not yet fully aligned their respective security programs with DHS' overall policies, procedures, and practices. For example, DHS cannot effectively manage its information security program while lacking an accurate and complete system inventory. The CISO has developed a formal inventory methodology based on federal guidance including FISMA and National Institute of Standards and Technology publications. Currently, the CISO has a team visiting OEs to facilitate inventory alignment based on the methodology. Further, as reported in our FY 2003 security program evaluation, DHS' OEs are not ensuring that IT security weaknesses are included in their Plan(s) of Action and Milestones (POA&M). To address this issue the CISO has implemented POA&M assist visits with each of the OEs, to better manage the entire POA&M process, including the identification and management of all security weaknesses.

In a separate report issued by the DHS OIG in June 2004, security controls were found to be inadequate and increase the risks to DHS wireless networks. The DHS OIG reported issues with wireless policy, procedures for wireless implementation, and effective oversight by DHS' National Wireless Management Office (WMO). The DHS WMO is working closely with the CISO to ensure that wireless security policy is properly formulated and promulgated, and is sufficient to ensure DHS' wireless communications. Department officials said that it will implement and maintain a rigorous certification and accreditation

⁴ The DHS CIO Council is comprised of the CIOs from each DHS component, ex officio representatives from General Counsel, the Chief Financial Officer's Council, the Office of the CIO, and the Executive Procurement Executive Council. The CIO Council was chartered to develop, promulgate, implement, and manage a vision and direction for information resources and telecommunications management within DHS.

(C&A) process for all wireless systems, personal electronic devices, and tactical wireless communication systems. Specifically, the Wireless Security Working Group within DHS will coordinate with the DHS WMO and DHS CISO to ensure consistency in the development and application of risk management approaches and C&A processes for wireless services and technologies. Department officials also said that this collaboration ensures the DHS WMO is effectively managing the department's wireless security risks. Additionally, the Designated Accrediting Authority within each organizational component will be responsible for approving the implementation and use of wireless systems at a specified risk level during the C&A process.

The department is also tasked to protect the nation's critical infrastructure from a major cyber terrorist attack. The DHS OIG reported in July 2004 that DHS has begun to implement the actions and recommendations detailed in *The National Strategy to Secure Cyberspace*. While a number of major initiatives have been undertaken, DHS still faces many challenges to address long-term cyber threats and vulnerabilities to the nation's critical infrastructure.

INFRASTRUCTURE THREAT ASSESSMENT

The department is tasked to protect the nation's critical infrastructure and national assets against terrorist attack. Before this assignment can be executed to its fullest, the IAIP directorate must identify and then compile the nation's critical infrastructure and national assets into a comprehensive National Assets Database (NADB). DHS has made progress on this task; as of July 2004, the NADB contained more than 33,000 national assets. However, the process the IAIP is using to assess the threats against those assets, determine how vulnerable they are to attack, ascertain their mitigation requirements, and prioritize the threat/mitigation effort is evolving. Presently, there is no blueprint for the NADB as no precedent exists for collecting such extensive information and making these difficult qualitative and quantitative assessments. Policies and procedures for maintaining the NADB are still in development. Although the IAIP provided guidance for the collection of data, the data it received was often inconsistent. The DHS OIG is evaluating the effectiveness and efficiency of the processes that the IAIP employs to develop and prioritize its inventory of the nation's key assets.

BORDER SECURITY

A primary mission of the DHS is to reduce America's vulnerability to terrorism by protecting the borders of the United States and safeguarding its transportation infrastructure. Within DHS, these responsibilities fall primarily with the Border and Transportation Security (BTS) Directorate.

Two organizations within BTS are responsible for enforcing the nation's immigration and customs laws. CBP inspects visitors and cargoes at the designated U.S. ports of entry (POE) and is responsible for securing the borders between the POEs. CBP's primary mission is to prevent terrorists and terrorist weapons from entering the United States, while also

facilitating the flow of legitimate trade and travel. ICE is the investigative arm of BTS that enforces immigration and customs laws within the United States. While CBP's responsibilities focus on activities at POEs and along the borders, ICE's responsibilities focus primarily on enforcement activities related to criminal and administrative violations of the immigration and customs laws of the United States, regardless of where the violation occurs. CBP and ICE have employees assigned outside the United States to protect the sovereignty of our borders.

Other organizations within DHS have border security related responsibilities. For example, the US-VISIT Program Office, also within BTS, is responsible for the development and fielding of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, DHS' entry-exit system. It also coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS). Also, USCIS is responsible for reviewing and approving applications for immigration benefits. While not a law enforcement agency, USCIS plays an integral part in DHS' border security program by ensuring that only eligible aliens receive immigration benefits and identifying cases of immigration benefit fraud and other immigration violations that warrant investigation or removal by ICE.

DHS faces several formidable challenges in securing the nation's borders. These include the development of an effective, automated entry-exit system (US-VISIT); disruption of alien smuggling operations; identifying, locating, detaining, and removing illegal aliens; fielding effective border surveillance technologies; integrating DHS' IDENT with the FBI's IAFIS fingerprint systems; providing timely, accurate, and complete intelligence to support border security operations; developing effective overseas operations; and, reducing the immigration benefit application backlog.

Tracking the Entry and Exit of Foreign Visitors

US-VISIT will provide the capability to record entry and exit information on foreign visitors who travel through United States air, sea, and land ports, and it will apply to non-immigrants holding non-immigrant visas. DHS thinks that the US-VISIT program will take five to ten years to implement fully its long term, comprehensive vision. To support US-VISIT in meeting its challenge, the US-VISIT Program Office awarded the prime integrator contract on June 1, 2004. The initial five-year contract, with one-year options for extension of another five years, is worth up to \$10 billion. Managing this mammoth project and associated budget will require considerable management and contractor oversight by DHS. The project has considerable risk, not only in terms of technology challenges that must be overcome, but the end product of the project is still undefined.

Alien Smuggling

Alien smuggling continues to be a major immigration problem in the United States. As border enforcement operations have made illegal entry into the United States more difficult, smugglers have profited. In addition to boosting their fees, smugglers have become

increasingly dangerous and aggressive in their tactics. ICE faces significant challenges in curbing these sophisticated and dangerous smuggling operations. ICE's limited resources have always been strained in its attempts to counter the economic magnet of the U.S. employment market. ICE reports that its Arizona Border Control Initiative led to a decrease in smuggling activity, the seizure of over \$5.3 million in smuggling assets, and the confiscation of 130 firearms.

Identifying, Locating, Detaining, and Removing Illegal Aliens

DHS continues to face challenges in identifying, locating, detaining, and removing aliens who have entered without inspection, violated the terms of their visas, or committed criminal acts. The current illegal alien population in the United States is estimated to be 8-12 million. ICE, the agency responsible for removing the illegal alien population, continues to wage an uphill battle to address this problem. ICE is hampered in part by shortages of special agents. It has approximately 5,500 special agents to cover the myriad of immigration and customs law enforcement responsibilities, of which locating illegal aliens is but one. ICE utilizes DHS non-immigrant registration systems, including the National Security Entry Exit Registration System (NSEERS), the Student and Exchange Visitor Information System (SEVIS), and US-VISIT to assist in the process of identifying and locating visa overstays and student status violators.

Further, ICE has the responsibility to detain certain illegal aliens until they are removed from the United States. With increasing frequency, ICE has been forced to weigh its detention decisions against budgetary constraints. Prior reports have shown the importance of detention in relation to the eventual removal of an alien. Hence, effective management of BTS detention space can substantially contribute to immigration enforcement efforts.

Advanced Border Surveillance Technology

CBP is challenged to monitor illegal immigration activity along remote and rugged stretches of the U.S. border with Mexico and Canada. Even if additional Border Patrol agents were available, officers alone cannot effectively monitor some border regions. CBP has employed technology to enhance border surveillance and its ability to detect illegal immigration activity. The technology includes the American Shield Initiative (ASI) and unmanned aerial vehicles. The challenges for CBP are to identify effective technologies; deploy the technologies appropriately; and integrate effectively those technologies as "force multipliers" into its border enforcement strategy.

Integrated Fingerprint Systems

DHS must move rapidly to complete the deployment of the integrated IDENT/IAFIS workstations to the border. Immigration authorities have long recognized the need for an automated fingerprint identification system to determine quickly the immigration and criminal histories of aliens apprehended at or near the border. Immigration authorities need to be able to determine quickly which aliens should be detained for prosecution based on membership in a terrorist organization, multiple illegal entries, re-entering the United States

after a prior deportation, alien smuggling, a current arrest warrant, or an aggravated criminal record.

In FY 1989 Congress provided the initial funding to develop an automated fingerprint identification system that eventually became known as IDENT. While IDENT was developed to meet identification purposes, the FBI developed its own fingerprint system, IAFIS, to meet its own requirements. Beginning in 1998, the need to integrate the two systems was recognized. IDENT could not interface with the FBI's fingerprint system, which prevented immigration authorities from obtaining criminal histories of aliens they had in their custody. In FY 1999, Congress mandated the integration of IDENT and IAFIS. The Department of Justice (DOJ) was originally given the responsibility for integrating the systems and was funded through annual appropriations. In FY 2004, despite not receiving funding, DHS was given responsibility for continuing the deployment of the IDENT/IAFIS capability. In addition, FY 2005 appropriations language tasks DHS to take the lead on future development of any integrated IDENT/IAFIS capability. DHS will be required to submit a report on the status of this effort, including steps the department will take to integrate IAFIS into IDENT, funds needed, and a timetable for full integration.

The integration project was started in 2000 with studies to be performed by DOJ on the impact of deploying an integrated IDENT/IAFIS capability. The first published schedule called for a limited integrated capability to be developed and deployed to selected sites by late 2002. Various delays and changes in project scope pushed out DOJ's schedule. Only a small percentage of sites had the capability by the beginning of FY 2004. To date, initial integrated workstations exist at all Border Patrol locations and most of the major ports of entry. Department officials said that the integrated workstation will allow a field agent to take a single set of fingerprints and simultaneously query both IDENT and IAFIS in real time, and that deployment to the remaining POEs and all interior locations should be completed in 2005.

The DOJ OIG reported in January 2004 that all aliens apprehended by the Border Patrol still are not checked against FBI criminal fingerprint records. Additionally, the FBI and other law enforcement agencies using the FBI's fingerprint records still cannot access DHS' criminal alien fingerprint records. The transfer of immigration responsibilities to DHS has created additional issues relating to the management of the integration project between DHS and DOJ. According to the DOJ OIG, unresolved issues include: (1) project leadership and responsibilities between DHS and DOJ; (2) funding; (3) technical interoperability issues between US-VISIT and IAFIS; (4) the development of integration project schedules; and (5) fingerprint image quality concerns.

Intelligence Support for Border Security Operations

Integrating the multiple data systems to compile a complete border security picture without requiring queries of multiple systems by ICE and CBP officers will be a major challenge. In order for CBP and ICE officers to identify potential threats to the security of the United States, whether it be persons or cargoes, they must be able to access all relevant information and intelligence from all sources regarding persons, vehicles, vessels, aircraft, criminal histories, travel records, etc. Officers must be able to access quickly information to develop

a complete picture of the current border security situation so that they can make appropriate enforcement decisions. Quick access to information is also vital to CBP's objective of facilitating legitimate travel and trade. However, officers must now conduct time consuming and difficult multiple database searches because systems are not integrated. The systems that they use are antiquated and not easily operated. Data displays are not always clear and officers could miss or overlook important information. Data within the systems cannot always be manipulated to conduct in-depth analysis to discern trends and patterns of illegal activities.

Efforts are currently ongoing to consolidate the various terrorist watch list systems used by federal agencies, and thereby help improve intelligence support for border security operations. According to the Homeland Security Act of 2002, DHS is to play a major role in watch list consolidation activities. However, these consolidation activities are still conducted by the federal organizations that were primarily responsible for collecting and disseminating terrorist information prior to DHS' formation.

International Operations

DHS faces international challenges in protecting our borders. Provisions in the visa issuance process and other programs to promote international travel create potential security vulnerabilities that may allow terrorists, criminals, and other undesirable travelers to enter the United States undetected.

For example, DHS must address security concerns identified in the Visa Waiver Program (VWP). The VWP enables citizens of 27 countries to travel to the United States for tourism or business for 90 days or less without obtaining a visa. These travelers are inspected at a U.S. POE, but have not undergone the more rigorous background investigations associated with visa applications.

BTS needs to strengthen and improve the management of the VWP, including issues related to lost and stolen passports (LASP). LASP information provided by VWP governments has not been thoroughly checked by the former INS or now by BTS against U.S. entry and exit information to determine whether the passports have been used to enter the United States. Collection of LASP data from VWP governments is not proactive or uniform. Further, LASP problems are complicated by the lack of international standardization in passport numbering systems that can result in a failure to identify *male fide* (in bad faith) travelers using stolen VWP passports even when the theft has been reported. The OIG recommended that US-VISIT biometric processing be extended to VWP travelers, a program change that DHS has adopted.

DHS must also address issues identified with its visa security program (VSP). The VSP stations DHS officers at U.S. embassies and consular offices overseas to review visa applications and perform other law enforcement functions. The VSP program received partial funding in FY 2004 and full funding in FY 2005. Because BTS has been compelled to use temporary duty officers who have not received training in foreign languages, they do not have these skills, and lacked adequate administrative support as well. As a result, the full

intelligence and law enforcement value that Visa Security Officers could add to the existing inter-agency country teams has not been achieved.

CBP has started a new program, the Immigration Security Initiative (ISI), to station CBP officers in foreign airports. The ISI officers are to interdict terrorists, illegal aliens, alien smugglers, and other criminals before they board U.S.-bound flights. As with any new initiative, CBP is faced with several challenges in establishing and managing this new program. First, adequate funding must be provided. Second, the officers working in the foreign airports must have adequate technical and administrative support to perform their missions. This includes connectivity to electronic database systems, which could be problematic in a foreign facility. Third, CBP must develop a cadre of specially trained officers that it can rotate into these positions.

Immigration Benefit Application Backlog Reduction

USCIS is challenged with processing immigration benefit applications and petitions in a timely manner. As of May 2004, USCIS had pending 5,696,066 applications and petitions. Of these, 233,696 were for asylum; 671,707 for naturalization; and 4,790,663 for immigration benefits. The Administration announced the aim of meeting a six-month standard from start to finish for processing applications for immigration. The President pledged \$500 million over five years, beginning with \$100 million requested for fiscal year 2002, to support USCIS in eliminating the backlog by the end of 2006.

USCIS issued a “Backlog Elimination Plan” in June 2004 that reframed how USCIS counts the backlog and proposed the following backlog elimination strategies: (1) new management tools; (2) improved processes and procedures; and (3) better use of technology. USCIS’ backlog reduction plan is ambitious and is based on numerous assumptions about application receipts, increased productivity, and the success of some pilot programs currently being conducted. Many of these assumptions would be severely disrupted if global immigration patterns or U.S. immigration law encountered significant changes. For example, a proposed new guest worker program would permit many currently illegal aliens to apply for some form of immigration status. If USCIS were suddenly inundated with potentially millions of unexpected immigration benefit applications, its efforts to eliminate current backlog would be severely hindered.

TRANSPORTATION SECURITY

Airport Screeners

The Aviation and Transportation Security Act (ATSA), which was enacted as a result of the events of September 11, 2001, mandated that the TSA hire and train thousands of screeners for the nation’s 429 commercial airports by November 19, 2002. As a result, TSA hired 62,000 screeners. A DHS OIG undercover audit of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not being carried into the sterile areas of heavily used airports or do not enter the checked

baggage system. Four areas caused most of the test failures and were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA is enhancing its screener training programs along with management and supervision of screener activities. The DHS OIG is evaluating TSA's revised training programs and will continue to monitor TSA's progress in improving screeners' performance.

Checking for Explosives

TSA has been largely successful in its effort to implement the ATSA requirement that all checked bags be screened by explosives detection systems (EDS). However, deployment of the equipment does not ensure effective security. Several OIG reviews have reported that TSA has not resolved the problems that arise when explosive detection equipment breaks down, there are workforce shortages, or high baggage volume overloads the system. Fallback alternatives are inconsistently applied and inadequately controlled, leaving gaps in the screening process. Also remaining to be done are: (1) deploying such equipment to the remaining airports where alternative screening methods are in use today; (2) integrating explosives detection systems into baggage handling systems at the largest airports (at a cost of more than \$3 billion); and, (3) using research and development funds to develop and deploy more effective and economical equipment to address current and future threats and risks. Additional safeguards are also needed to screen and inspect cargo transported on passenger aircraft.

Recently, TSA has come under criticism from both members of Congress and the 9/11 Commission for not moving quickly enough to address the vulnerability of the nation's air traffic to suicide bombers. Specifically, TSA has not installed explosives detection technologies at the checkpoint to screen for explosives on the body. TSA is in the process of testing several of these technologies that include backscatter x-ray, vapor detection, and document scanner machines to address concerns regarding detection of explosives on individuals. TSA is currently piloting explosives trace detection document scanners at four airports to assess the viability and effectiveness of the technologies.

DHS OIG is continuing to monitor TSA's progress regarding these issues as well as reviewing TSA's process for screening air cargo.

Maritime Security

The U.S. Coast Guard is the lead DHS agency for maritime homeland security, and is responsible for developing and implementing a comprehensive National Maritime Transportation Security Plan to deter and respond to transportation security incidents. The marine areas under U.S. jurisdiction cover 3.5 million square miles of ocean, 95,000 miles of coastline, and 26,000 miles of commercial waters serving 361 domestic ports. These activities account for two billion tons and \$800 billion of domestic and international freight annually. Approximately 8,000 foreign vessels, manned by 200,000 foreign sailors, make more than 50,000 ship visits to U.S. ports each year.

The Coast Guard faces significant management challenges. The most daunting challenges include restoring the Coast Guard's readiness to perform its legacy missions; implementing the Maritime Transportation Security Act of 2002 (MTSA); maintaining and replacing the Coast Guard's deepwater fleet assets; and developing adequate infrastructure needed to support the Coast Guard's multiple missions.

Readiness to Perform Coast Guard Legacy Missions

The Coast Guard faces three major barriers to improving and sustaining its readiness to perform its legacy missions. First, the lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance. The Coast Guard has yet to comprehensively define a performance management system that includes all the input, output, and outcomes needed to gauge results and target performance improvements, balance its missions, and ensure the capacity and readiness to respond to future crisis or major terrorist attacks. Second, the workload demands on the Coast Guard will continue to increase as it implements MTSA. This complex work requires experienced and trained personnel; however, the Coast Guard has in recent years suffered from declining experience levels among its personnel. Third, sustaining a high operating tempo due to growing homeland security demands, such as added port, waterway, and coastal security patrols, will tax the Coast Guard's infrastructure including its aging cutter and aircraft fleet.

Implementing MTSA

The Coast Guard faces challenges in fully implementing MTSA and enforcing the required vessel, facility, and area security plans. MTSA regulations affect approximately 9,200 vessels, 3,200 port facilities, and 40 offshore terminals. Owners and operators of vessels, facilities, and terminals were required to develop port security plans consistent with Area Maritime Security Plans. Vessel and facility plans were reviewed and approved by the Coast Guard, and implemented by July 1, 2004. The Coast Guard, working through Captains of the Port, is working to develop and implement 43 Area Maritime Security Plans covering the Nation's 361 seaports. These plans are to be implemented in concert with the national security and homeland defense strategies and plans. The Coast Guard must ensure that these plans are effectively implemented, including its key and unique role of ensuring the MTSA regulations are enforced.

In addition, the Coast Guard must identify, target, track, board, inspect, and escort high interest vessels that may pose a substantial risk to U.S. ports due to the composition of the vessel's crew, passengers, or cargo. The Coast Guard has instituted strict reporting requirements for all vessels arriving at U.S. seaports, mandating most commercial vessels to provide a 96-hour Advance Notice of Arrival. Certain vessels operating on U.S. navigable waters must also be equipped with and operate an Automatic Identification System (AIS), which includes a position indicating transponder. The Coast Guard has also developed a sophisticated decision-making system for targeting high interest vessels, cargoes, and crews. The Coast Guard faces a major management challenge to validate and fully implement these targeting procedures.

Maintaining and Replacing Deepwater Assets

In June 2002, the Coast Guard awarded a \$17 billion contract to maintain and replace its Deepwater assets. This contract called for replacing or modernizing, by 2022, all assets used in missions that primarily occur more than 50 miles offshore, including approximately 90 cutters, 200 aircraft, and assorted sensors and communications systems. According to the Coast Guard, the greatest threat to its ability to safely and effectively perform its assigned missions continues to be the operational capability of its legacy aircraft, cutter, and small boat fleet. These assets are aging and are becoming more difficult and expensive to maintain. In some instances, the Coast Guard is experiencing difficulty maintaining and upgrading existing critical deepwater legacy assets including the HH-65, HH-60, HC-130 aircraft and its coastal patrol boat fleets.

Maintaining the operational readiness of critical legacy assets is a major challenge to the Coast Guard. As an example, the rate of in-flight loss of power mishaps involving the HH65 helicopter far exceeds FAA and U.S. Navy safety standards, requiring the immediate re-engining of the entire HH65 fleet. The Coast Guard estimates that sustaining its deteriorating legacy assets will escalate to \$140 million in fiscal year 2005, further challenging the Coast Guard to rethink plans and schedules for maintaining or replacing legacy assets.

Revisiting maintenance, upgrade, and replacement decisions for legacy assets may disrupt the Deepwater contractor's plans and schedules and, therefore, could greatly increase future program costs. For example, the Coast Guard must diligently monitor the schedule and costs for maintaining, renovating, or upgrading its coastal patrol boats and medium and high endurance cutters. Revisiting these decisions may be prudent, considering the adverse impact deteriorated fleet conditions are having on Coast Guard mission performance. In 2003, the Coast Guard experienced 676 unscheduled maintenance days for its cutters—a 41% increase over 2002. This was the equivalent of losing the services of over three and a half cutters. These lost cutter days include the coastal patrol boats that are suffering from accelerated hull corrosion and breached hull casualties.

Infrastructure in Support of Coast Guard Missions

The Coast Guard Acquisition, Construction, and Improvement (AC&I) budget requests during FY(s) 2003-2005 did not include adequate funding for the re-capitalization of critical infrastructure. For example, the Coast Guard requested only \$5.5 million for shore side infrastructure during FY 2004. This infrastructure must be planned, designed, funded, and constructed in time to support properly the Deepwater boats, cutters, and aircraft, as well as their crews. The lack of infrastructure funding could be a major detriment to the Coast Guard's ability to perform both its legacy and homeland security missions.

Other Transportation Modes

While TSA continues to address critical aviation security needs, it is moving slowly to improve security across the other modes of transportation. About 6,000 agencies provide

transit services through buses, subways, ferries, and light-rail services to about 14 million Americans. Recently, several congressional leaders expressed concern that the federal government has not taken strong enough action to respond to the threat to passenger and public transit. Furthermore, the 9/11 Commission recently reported that over 90% of the nation's \$5.3 billion annual investment in TSA goes to aviation, and that current efforts do not yet reflect a forward-looking strategic plan systematically analyzing assets, risks, costs, and benefits so that transportation security resources can be allocated to the greatest risks in a cost effective way.

TSA has lead responsibility for coordinating development of a transportation sector plan, which should be completed by the end of the year. TSA, however, has not finalized the memorandums of understanding with various Transportation Department agencies to determine how they will coordinate work in the future.

DHS OIG is evaluating TSA's actions to assess and address potential terrorist threats to the mass transit systems of major U.S. metropolitan areas.

Management's Response to the Inspector General's Statement on the Top Management Challenges Facing the Department of Homeland Security

The Department recognizes the challenges identified by the Inspector General (IG) and the potential impact the challenges could have on the effectiveness and efficiency of department programs and operations if not properly addressed. In most cases, the IG's statement identifies the priority actions the Department is taking to address these challenges, many of which have been completed or are currently in progress. This is especially so in light of the fact that the fieldwork associated with the Office of the Inspector General (OIG) Report's underlying reviews was completed many months ago. The Department anticipates that the results of initiatives to address the management challenges during fiscal year 2005 and a reassessment of other challenges should enable the IG to report formidable progress next year. Some challenges, however, require legislative action or necessitate that actions be taken jointly with non-Department of Homeland Security government agencies.

Where a sustained effort is required over several years to address an OIG management challenge that impacts a core program or management priority, performance goals and strategies will be developed at either the Departmental or agency level and included in annual performance plans. For example, plans at the Departmental and agency level are in place to comprehensively address management challenges such as integrating information systems and issues on border and transportation security identified in the IG's statement. These long-term plans will be reflected in the Department's *Future Years Homeland Security Program*.

The following provides additional information to amplify or clarify the corrective actions identified in the IG report:

Consolidating the Department's Components

During the first 20 months of existence, the Department has accomplished the largest reorganization of the Federal Government in more than half a century. This task, creating the third largest cabinet agency with the critical, core mission of protecting the country against another terrorist attack, has presented many challenges, which are being met by the Department's managers and employees. The Department recognizes there is yet much to be done and is taking those steps crucial to integrating and consolidating the various components of the Department.

The Department is integrating and streamlining the support service functions directly accountable to the functional Line of Business (LOB) Chiefs such as the Chief Procurement Officer (CPO), Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Human Capital Officer (CHCO) and Chief of Administrative Services (CAS). The LOB Chiefs have developed Management Directives to guide the Department's management of that business function and are now implementing systems to optimize their functions across the entire Department. The systems are based on "dual accountability" where both the operational leadership and the LOB chiefs are responsible for the successful implementation of the directives. The Management Directives provide direction for both process and resource management. The Secretary signed these documents in October to institutionalize the arrangements before fiscal year 2005.

Contract Management

Overall, the Department is taking positive steps to build and improve the Department's contract management system. To help address the issues raised by the OIG, the Department formed the Office of Procurement Operations (OPO) to provide procurement support for components without an indigenous contracting capability. To help bridge the staffing gap, the Department contracted with other federal agencies to provide contract management support. The OPO has developed a staffing plan to bring OPO's staffing level to 127 by the end of fiscal year 2005. The cost of these positions will be funded through the Working Capital Fund.

The Department's efforts to provide a sufficiently detailed and accurate listing of procurement information proved difficult and were hampered by legacy federal systems. While it has migrated all of its procurements under the umbrella of one comprehensive reporting system, the Department still lacks sufficiently detailed and validated data for fiscal year 2003 and fiscal year 2004 to manage the procurement universe and ensure accurate and consistent reporting.

To help ensure large, complex, high-cost procurement projects are closely and properly managed, the Department has implemented a vigorous Investment Review Process (IRP) that:

- Integrates capital planning and investment control, resource allocation, budgeting, acquisition, and management of information technology and non-information technology investments to ensure scarce public resources are wisely invested and operational requirements are met.
- Ensures that spending on investments directly supports and furthers the Department's mission and provides optimal benefits and capabilities to stakeholders and customers.
- Identifies poorly performing investments that are behind schedule, over budget, or lacking in capability so corrective actions can be taken.
- Identifies duplicative efforts for consolidation and mission alignment when it makes good sense or when economies of scale can be achieved.
- Improves investment management in support of the President's Management Agenda.

To date, over 75 percent of the Department's major investments have been reviewed by the Investment Review Board (IRB) or the Joint Requirements Council.

Financial Management

We acknowledge the significant financial management challenges facing the Department of Homeland Security and we are committed to work with the OIG to establish a world-class financial management program. Between our inaugural and second year of operations we have demonstrated resolve and have:

- Steadily improved the involvement of component level financial management resources.
- Hired a diverse set of financial management expertise in the areas of accounting systems, the U.S. Standard General Ledger, financial reporting, and internal controls.
- Partnered with private sector consultants to produce standard operating procedures that will promote consistent, timely, and accurate consolidated financial reporting in compliance with Federal accounting standards and control requirements.

We are firmly committed to accountability and embrace the *Department of Homeland Security Financial Accountability Act*. In fiscal year 2005, we will approach financial management "methodically; building our financial management infrastructure right is more important to us than rushing to an outcome." We are already proactively engaged in numerous activities to better our financial management processes. In fiscal year 2005 we will:

- Integrate financial management functions to achieve our goal of a functionally integrated Department.
- Continue to use public and private sector partnerships to prepare standard financial management operating policies and procedures. We are utilizing best-in-class financial management policies and procedures to assist in expediting our efforts in this area. This will set the financial management internal control framework for the Department.
- Launch implementation of a strategy to transform legacy internal control structures into a Departmental internal control structure.
- Conduct an operating risk assessment of our financial reporting processes. The assessment will provide a gap analysis to identify the key risks over Departmental financial reporting and an inventory of internal control issues to enable us to close control gaps.

The Office of the Chief Financial Officer (OCFO) is pursuing an efficient and integrated approach that builds on government, industry, and project management best practices for acquiring a commercial off-the-shelf financial management package and the system integration expertise necessary for implementation. This approach called eMerge² will use a performance-based acquisition strategy based on effective planning and requirements-gathering consistent with department information technology policy and system development life-cycle guidance. OCFO is managing eMerge² using critical components of earned-value management methods for program planning, reporting, and management. OCFO has also developed appropriate planning documents, emphasizing different aspects of the effort, to ensure that the acquisition and implementation of a modern financial management system is cost-effective, efficient and meets the Department's business, technical and compliance needs.

Integration of Information Systems

Creating a single infrastructure for effective communications and information exchange is a major management challenge for the Department. The CIO is developing the strategies and technologies needed to connect the local, metropolitan, and wide area networks of the Department's legacy agencies.

The Department's CIO is an integral member at each level of the information technology investment review process. The Department's CIO heads the CIO Council (comprised of all CIOs across the Department) and the Enterprise Architecture Board and is a key member of the IRB as part of the Department's IRP. The IRB is the executive review board that provides acquisition oversight of the Department's major investments. The IRB is the forum that provides senior management the proper visibility, oversight, and accountability for major investments whether they are information technology or non-information technology. It also serves as a forum for discussing investment issues and resolving problems requiring senior management attention.

Maritime Security

The Coast Guard continues to improve a robust mission program performance management system and readiness to perform legacy missions in close coordination with the Department and OMB on Program Assessment Rating Tool reviews and independent program evaluations. Further refinement of the Coast Guard's comprehensive performance management system will include alignment and measurement of activities that contribute to department and Coast Guard agreed upon outcomes. This will further enable the Coast Guard to gauge results and target performance improvement, balance its missions, and ensure the capacity and readiness to respond to future crisis or major terrorist attacks. Coast Guard leadership is also proactively engaged in periodic long-term scenario planning to foresee future needs. For example, the Coast Guard is preparing a comprehensive schedule that will include the current status of its Deepwater Project asset acquisition phases (such as concept technology and design, system development and demonstration, and fabrication), interim phase milestones (such as preliminary and critical design reviews, installation, and testing), and the critical paths linking the delivery of individual components to particular assets.

The Coast Guard, in coordination with its industry partner, Integrated Coast Guard Systems, is analyzing repair or replace decisions for some assets. These analyses are being conducted primarily to ensure that the Coast Guard achieves operational requirements and does not suffer reduced asset capability. Additionally, an increase in cost is not necessarily a result. In some cases proposed changes will result in savings.

Heritage
Special Report

SR-02
DECEMBER 13, 2004

 Published by The Heritage Foundation

DHS 2.0: Rethinking the Department of Homeland Security

James Jay Carafano, Ph.D.
David Heyman

James Jay Carafano, Ph.D., is Senior Research Fellow for Defense and Homeland Security in the Kathryn and Shelby Cullom Davis Institute for International Studies at The Heritage Foundation.

David Heyman is Director and Senior Fellow of the Homeland Security Program at the Center for Strategic and International Studies.

The task force co-chairmen and participants would like to acknowledge the helpful support provided by the Center for the Study of the Presidency and the use of its online Homeland Security Database and Information Exchange Site, which facilitated the task force's deliberations. The site is located at www.thepresidency.org/hsdatabase.htm.

© 2004 by

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002-4999
(202) 546-4400 • heritage.org

and

The Center for Strategic and International Studies
1800 K Street, NW
Washington, DC 20006
(202) 887-0200 • www.csis.org

Table of Contents

Executive Summary	5
Introduction	7
I. Management	11
<i>Management of Operations</i>	
<i>Policy Formulation and Implementation</i>	
<i>Human Capital Management (Personnel Programs)</i>	
<i>International Affairs</i>	
<i>Integrating Operations with Non-Federal Entities</i>	
II. Roles and Missions	15
<i>Border, Immigration, and Transportation Security</i>	
<i>Critical Infrastructure Protection, Preparedness, and Response</i>	
<i>Intelligence Analysis</i>	
III. Authorities	19
<i>Department Oversight</i>	
<i>Information Sharing and Technology Development and Acquisition</i>	
<i>Protection of Sensitive, but Unclassified Information</i>	
<i>Clarification of Authorities for Critical Missions</i>	
<i>Watchlists, Profiling, and Policies for Information Protection</i>	
IV. Resources	23
<i>Authorization Process</i>	
<i>Allocation of Grants</i>	
<i>National Threat/Vulnerability Assessments</i>	
<i>Response to Catastrophic Terrorism</i>	
<i>Border Security</i>	
Task Force Participants	27

Executive Summary

This report presents the conclusions of a task force charged with examining the organization and operations of the U.S. Department of Homeland Security (DHS). The task force included representatives from academia, research centers, the private sector, and congressional staff and was chaired by homeland security experts from the Center for Strategic and International Studies and The Heritage Foundation. The task force evaluated DHS's capacity to fulfill its mandate as set out in the Homeland Security Act of 2002 based on four criteria: management, roles and missions, authorities, and resources.

Based on this analysis, conducted through seminars, an extensive literature search, and interviews, the task force developed over 40 major recommendations. Together, these proposals make the case for a significant reorganization of the department to make it a more effective and efficient instrument for preventing and responding to terrorist threats.

Each section consists of findings and recommendations agreed upon by the task force. Major recommendations in the report include:

- **Strengthening** the Secretary of Homeland Security's policymaking function by creating an Undersecretary for Policy.
- **Empowering** the secretary by establishing a "flatter" organizational structure through (1) consolidating and strengthening agencies with overlapping missions; (2) eliminating middle-management (director-ate) layers over border and transportation security, preparedness and response, and information analysis and infrastructure protection; and (3) having the agencies report directly to the secretary via the Deputy Secretary of Homeland Security.
- **Rationalizing** government spending by establishing a risk-based mechanism for department-wide resource allocation and grantmaking and by developing pre-determined "response packages" to respond to catastrophic terrorism.
- **Clarifying** authorities and national leadership roles for bio-defense, cyberdefense, and critical infrastructure protection.
- **Improving** departmental oversight by rationalizing congressional committee structure and establishing permanent oversight committees in the House of Representatives and the Senate.

Congress and the Administration should develop a comprehensive plan to restructure the department, including establishing a nonpartisan commission to review the performance of the department and assess its capacity to fulfill the missions outlined in the Homeland Security Act in the areas of management, missions, authorities, and resources and to report back within six months.

Introduction

On November 25, 2002, the Homeland Security Act of 2002 transferred over 22 federal entities—some intact and some in part—and 180,000 employees into the newly created U.S. Department of Homeland Security (DHS). According to the legislation, the department's mission is (1) to prevent terrorist attacks within the United States, (2) to reduce the vulnerability of the United States to terrorism, and (3) to minimize the damage and assist in the recovery from terrorist attacks that do occur within the United States. Created as part of the national response to the horrifying terrorist attacks on New York and the Pentagon on September 11, 2001, DHS is the single most ambitious and sweeping bureaucratic initiative undertaken by the federal government to protect Americans against future terrorist threats.

This report assesses progress in that effort. A task force representing academia, research centers, the private sector, and congressional staff chaired by homeland security experts at the Center for Strategic and International Studies and The Heritage Foundation examined the effectiveness of the new department in four areas: management, roles and missions, authorities, and resources. Based on this analysis, conducted through seminars, an extensive literature search, and interviews, the task force developed 40 major recommendations for improving the oversight, organization, and operation of DHS.¹ We believe that, taken together, these recommendations make the case for a significant reorganization of the department to empower the Secretary of Homeland Security and make the department a more effective and efficient instrument for preventing and responding to terrorist threats.

Why This Report? Why Now?

We have learned a lot since 9/11. In the three years following the most serious attacks on U.S. soil since Pearl Harbor, Americans have had ample time to dwell on the challenges of protecting the nation against foreign threats in the 21st century and to review the efficacy of our response to these dangers. The results of both efforts suggest that it is time to rethink the place of the Department of Homeland Security in this effort.

There are no frontiers in 21st century national security. Distinguishing clear lines of responsibility between foreign and domestic security is a thing of the past. Additionally, the age when only great powers could bring great powers to their knees is over. The specter of catastrophic terrorism that could threaten tens of thousands of lives and hundreds of billions of dollars in destruction will be an enduring concern. A review of the initial conception for DHS in the Homeland Security Act suggests that the department's original organization does not reflect these realities well.

Putting it bluntly, the current organization of DHS must be reformed because it hampers the Secretary of Homeland Security's ability to lead our nation's homeland security efforts. The organization is weighed down with bureaucratic layers, is rife with turf warfare, and lacks a structure for strategic thinking and policymaking. Additionally, since its creation, whether one looks at the department's capacity to organize and mobilize a response to a catastrophic terrorist attack or at the international dimension of DHS programs, the department has been slow to overcome the obstacles to becoming an effective 21st century national security instrument.

A new threat environment requires a new approach to security. A nimble, highly adaptive adversary necessitates a bureaucracy that is flexible and responsive to a constantly changing threat. The melting of borders and blurring of foreign and domestic interests means that we need to foster new working relationships at home and abroad. The two lead agencies charged with protecting America are the Department of Defense (DOD) and the Department of Homeland Security. If the Department of Defense has been a primarily outward-looking institution, it must now provide greater support to domestic security. If the Department of Homeland Security has been primarily inward-focused, it must now also embrace the international dimensions of security, especially given the globally interconnected networks of our global society.

1. To the greatest extent possible, this document reflects a consensus of the task force members. However, not all members of the task force agreed with each and every recommendation. This document and all of its recommendations are intended to initiate a dialogue and to provide options for consideration by those in Congress and the executive branch responsible for protecting America.

It is not prudent to wait much longer before addressing this issue. Experience reminds us that it takes only a few years for a bureaucracy to become entrenched. After that, it becomes nearly impossible to change. The creation of the Department of Defense is a case in point. In the debates over the 1947 National Security Act and again as President, General Dwight D. Eisenhower lobbied for reorganizing the Pentagon to ensure that Army, Navy, Marine, and Air Force assets would work closely together. However, he failed to overcome the political opposition and service parochialism that blocked reforms. As a result, fundamental problems in joint operations went unaddressed until passage of the Goldwater–Nichols Act in 1986. The lesson is clear: Fix it at the beginning or live with the mistakes for a long time.

Organization of the Report

The task force's conclusions are organized into four parts that address the key areas that affect how well the organization and operations of DHS fulfill the department's mandate as defined in the Homeland Security Act:

- **Management** considers the organization and functions of the DHS secretariat and their capacity to integrate and effectively direct departmental activities and to provide a coherent vision for the future.
- **Roles and Missions** presents findings and recommendations concerning the organization and conduct of operations for the department's most critical security tasks.
- **Authorities** addresses the adequacy of the legal authorities and policies governing significant department activities.
- **Resources** looks at limitations on the department's ability to allocate resources efficiently and respond effectively to critical missions.

Major Recommendations

Each section consists of findings and recommendations agreed upon by the task force. The findings are what we believe to be significant statements of fact that describe and explain the department's performance. The recommendations are measures that the task force proposes that the Administration and Congress undertake to improve the organization and operation of the department. The recommendations are not intended to be comprehensive. They represent what the task force felt were the highest-priority initiatives. Major recommendations in the report include:

- **Strengthening** the Secretary of Homeland Security's policymaking function by creating an Undersecretary for Policy.
- **Empowering** the secretary by establishing a "flatter" organizational structure through (1) consolidating and strengthening agencies with overlapping missions; (2) eliminating middle-management (director-ate) layers over border and transportation security, preparedness and response, and information analysis and infrastructure protection; and (3) having the agencies report directly to the secretary via the Deputy Secretary of Homeland Security.
- **Rationalizing** government spending by establishing a risk-based mechanism for department-wide resource allocation and grantmaking and by developing "response packages" to respond to catastrophic terrorism.
- **Clarifying** authorities and national leadership roles for bio-defense, cyberdefense, and critical infrastructure protection.
- **Improving** departmental oversight by rationalizing congressional committee structure and establishing permanent oversight committees in the House of Representatives and the Senate.

Next Steps

Addressing the task force's recommendations in a piecemeal manner would be wrong. None of these measures is individually sufficient to create the DHS that America needs for the future. Indeed, the efficacy of many of these

initiatives depends on the adoption of the others. Congress and the Administration should develop a comprehensive plan to restructure the department. The task force recommends the following agenda for reform.

- The first action of the 109th Congress should be to consolidate oversight and establish permanent committees in the House and Senate with jurisdiction over all of the homeland security responsibilities of the department.
- The President and Congress should establish a nonpartisan commission to review the performance of the department and assess its capacity to fulfill the missions outlined in the Homeland Security Act in the areas of management, missions, authorities, and resources and to report back within six months. The commission should hold public hearings in addition to its other deliberations and develop a specific and detailed reorganization proposal.
- As part of the process for developing recommendations, the President and Congress should establish principles to guide the commission's efforts.
- Congress should develop and pass a reorganization bill in the next succeeding session.

There is little room for complacency. The threat of transnational terrorism will be enduring. America needs a DHS that is well prepared for the long fight.

I. Management

Management of Operations

Findings. DHS represents a complex merger of many agencies, combined with a number of start-up activities and compounded by the lack of a pre-existing senior management team. The U.S. Government Accountability Office (GAO)² rated the management challenge facing the department as “high risk” and noted that the successful transformation of a large organization takes from five to seven years.

While DHS has made progress in rationalizing many basic operations, including finance, contracting, information technology, human resources, and grant management, many operations still lack adequate coordination. According to DHS’s Office of Inspector General (OIG), the department remains a “collection of separate components operating under a common organizational umbrella.”

The Undersecretary for Management adds an unnecessary layer of bureaucracy. Other key management officials—the Chief Financial Officer (CFO), the Chief Information Officer (CIO), and the Chief Procurement Officer (CPO)—who report to the undersecretary also lack effective department-wide authority. In the private sector, chief management officers such as a CFO or a CIO report directly to the company’s top executives, the chief executive officer or the chief operating officer (COO). Some federal agencies such as the Department of Energy follow this model. However, DHS does not.

Recommendations. The DHS Deputy Secretary should be invested with powers and responsibilities similar to those of a COO, and this role should be codified.

The authority of the management directorate should be strengthened. Options for accomplishing this include moving management responsibilities into the Office of the Deputy Secretary or having the department’s CFO, CIO, and CPO report directly to the secretary through the deputy secretary as proposed in the House version of the 2005 Homeland Security Appropriations Bill.

Clear policies and procedures must be established to ensure that the CFO and CIO comply with the requirements in the CFO Act and the Clinger-Cohen Act. These two acts aim to increase federal government efficiency, primarily through improving financial, acquisition, and information technology management practices.

Policy Formulation and Implementation

Findings. The DHS Secretary currently lacks a policy apparatus with which to lead the development of proactive, strategic homeland security policy, let alone do anything beyond “managing by the in-box” and responding to the crises of the day. DHS also currently lacks a high-level policy officer with the staff, authority, and gravitas to articulate and enforce policy guidance throughout and across the department. DHS needs a more substantial capability to provide guidance for integrating current efforts. When DHS was formed from dozens of existing U.S. government agencies and programs, it absorbed several legacy policy analysis units from its component agencies. In addition, the patent need for policy analysis led some DHS components to form their own small policy analysis units. The proliferation of policy centers within DHS has only magnified the challenge of forging coherent guidance.

Recommendations. DHS should establish a unified policy planning staff headed by an Undersecretary for Policy who would report directly to the secretary via the deputy secretary. The undersecretary would serve as the secretary’s chief policy official within the department. The responsibilities of the Undersecretary for Policy should be established by law and should include:

2. Formerly the U.S. General Accounting Office.

1. Coordinating DHS policy. The undersecretary would establish and direct a formal policymaking process for the department and oversee a policymaking board.
2. Conducting long-range policy planning. The undersecretary's staff would conduct long-range strategic planning, including "what if" scenario-based planning—a task that other DHS components invariably neglect as they grapple with daily crises and other pressing short-term demands.
3. Preparing critical strategic documents, such as a national strategy for preventing terrorists from entering the United States. The undersecretary's office would help to compose the department's most important documents.
4. Conducting program analysis. The undersecretary would assist with DHS programming. In particular, the undersecretary's analysts would evaluate ongoing and proposed programs (including planned research and development efforts) in terms of overall DHS priorities and resources.
5. Preparing net assessments. The undersecretary's planners would conduct periodic net assessments and research specific issues of interest to the secretary and other DHS leaders that cut across the department's components or for which the leadership desires another opinion.

Human Capital Management (Personnel Programs)

Findings. Beyond the numerous pressing short-term operational priorities, the department faces serious long-range challenges, including the development of a common vision, culture, and management philosophy that are necessary to align and integrate all the discrete parts of the organization. This means not only meshing the diverse operations and functions of those component parts, but also developing a new and fundamentally different leadership culture within the department: a challenge equal in magnitude—and importance—to all the immediate priorities facing DHS. Such an integration of vision and purpose is imperative if DHS is to realize its massive agenda.

Similarly, retaining and attracting the best personnel is one of the toughest challenges faced by organizations in the midst of reorganization and transition. During significant organizational change, productivity and morale suffer, as does cooperation among employees, particularly from different parts of an organization. DHS is no exception. For example, in the first year of DHS operations, turnover among divisional CIOs was 45 percent. Personnel turbulence within the Border and Transportation Security Directorate was also significant. Further, an August 2004 report from the Office of Management and Budget (OMB) found that DHS needed to reduce talent gaps in mission-critical positions.

Recommendations.

- Establish an executive leadership program. Higher priority must be given to establishing leader and personnel development programs for a more homogeneous and unified workforce across the department, both in terms of building a shared DHS culture and in developing the skills and attributes required to deal with the challenges of the 21st century. The department needs something similar to the requirements established for the Department of Defense by the Goldwater-Nichols Act of 1986, which prescribed education, interagency and interdepartmental assignments, and skill levels for senior leaders.
- Continue to build and strengthen human resources. Congressional action may be required to further reform personnel regulations to include management and skills-based education, and career incentives and rewards that support internal department "cross fertilization," interagency operations, innovation, and rewards for non-standard career paths that benefit the department.
- Develop innovative means to attract the right people. Institute a program of undergraduate and graduate scholarships that creates a pool of professional recruits from multiple disciplines. The program might be roughly modeled on the Department of Defense's Reserve Officer Training Corps program.
- Establish an aggressive mid-grade and senior-grade recruitment program to attract talent from the private sector.

- Create a manpower “float” that allows all agencies of the department to institute long-term education programs in support of DHS professional development goals.
- Enact regulations that hold sub-department agencies and leadership responsible for specific personnel goals and performance criteria.

International Affairs

Findings. The global networks that sustain our economy and foster our way of life—e.g., transportation, energy, communications, and finance—can be exploited by terrorists to attack us at home. In addition, adversaries could attack these globally integrated networks directly, causing major disruptions in the global economy. “Homeland” security activities in many areas—including ports and cargo, aviation, public health, visa and passport standards, and consular affairs—do not stop at America’s geographic borders and really must be viewed as “international” security activities. Such activities necessarily involve diplomatic intelligence, information sharing, and other cooperative activities within foreign countries.

Although DHS has established an Office of International Affairs (OIA) to set strategic direction for the department’s international activities, DHS international efforts remain fragmented among multiple offices, including the OIA, the Border and Transportation Security’s (BTS) Policy Office, and other agency policy and operational activities within Immigration and Customs Enforcement (ICE), Citizenship and Immigration Services (CIS), Customs and Border Protection (CBP), and the U.S. Coast Guard.

Because of this fragmentation (which reflects DHS’s overall incomplete integration), DHS is unable to present a unified effort and presence overseas. As a result, DHS remains disenfranchised from the foreign policy apparatus. Within embassies, DHS presence is ad hoc and its role, mission, and relationship with the rest of the embassy is unclear. Foreign governments that share security interests with the U.S. may fail to build effective partnerships because of the lack of a clear path to partnership. DHS is poorly represented among important international organizations, including the European Union and the Organization for Security and Cooperation in Europe, which could play extremely helpful roles in homeland security.

Recommendations.

- Reorganize responsibilities for international affairs in the secretariat.
- Eliminate redundancy of roles between the Chief of Staff’s office and the OIA.
- Realign all DHS-wide international policymaking activity under an undersecretary.
- Convert the position of OIA Director to an assistant secretary under the Undersecretary for Policy.
- Clearly delineate the key responsibilities of the Assistant Secretary for Policy (International Affairs). They should include: (1) coordinating policy regarding international activities among DHS agencies; (2) coordinating international visits of the secretary related to protocol issues, and (3) ensuring DHS representation in dealing with international institutions, including the United Nations, NATO, the EU, the International Maritime Organization, and the World Customs Organization.

Integrating Operations with Non-Federal Entities

Findings. It is improbable that a catastrophic terrorist attack would affect only a single city or that a single city would be sufficiently prepared to mount a sufficient response. At a minimum, response efforts would likely require mutual aid from multiple jurisdictions. Despite this, DHS lacks an effective regional structure to facilitate coordination with state and local governments and with the private sector. Although efforts such as the National Response Plan and the National Incident Management System are providing a framework for this activity, DHS still lacks a suitable operational structure to support them.

The Homeland Security Advisory System (HSAS) is an important component of the intelligence and early warning mission area. The HSAS employs a series of color codes to designate various levels of national preparedness in

anticipation of a terrorist attack. Associated with each threat condition are a range of suggested protective measures—such as implementing various contingency plans—with federal, state, and local agencies responsible for developing and implementing their own specific response activities.

Application of the HSAS to state and local governments, as well as to the private sector and the American public, is problematic. A survey of various state and local response organizations conducted by the Gilmore Commission showed overwhelmingly that these organizations want more information on the type of attack, where it is likely to occur, and when. Currently, few organizations have the classified intelligence and the sophisticated analytical capabilities to evaluate threats. Without concrete assessments, many states, counties, and cities typically react in two ways: doing nothing or piling on layers of possibly unneeded security that generate exorbitant overtime costs and other expenditures.

Of even greater concern is the impact of shifts in the threat level on average citizens. Many appear perplexed by changes in threat condition. In short, the current national homeland security advisory system is inadequate.

Recommendations.

- Consolidate DHS critical infrastructure protection, preparedness, and state/local/private coordination efforts under an Undersecretary for Protection and Preparedness. This would consolidate the following agencies, components, and authorities: (1) the Infrastructure Protection component of the Information Analysis and Infrastructure Protection Directorate; (2) the Office of State and Local Government Coordination and Preparedness; (3) the non-operational transportation infrastructure protection mission of the Transportation Security Administration (TSA); (4) the "preparedness" piece of the Emergency Preparedness and Response Directorate; (5) the private sector preparedness mission of the Office of Private Sector Liaison; and (6) DHS grantmaking authority. Consolidating these disparate efforts would provide the DHS Secretary with a stronger platform from which to lead national efforts, determine priorities, identify critical vulnerabilities, work with state/local/private sector entities on securing those vulnerabilities and preparing for attacks, and make grants to help get the job done and to induce cooperation.
- Construct a DHS regional structure. The first priority of this regional organization should be to support the flow of information and to coordinate training, exercises, and professional development for state and local governments and the private sector. The regional structure's key operational mission would be to support preparedness, response, and critical infrastructure protection. DHS regional directors should not have authority over existing DHS agencies (such as the Coast Guard or Customs and Border Protection Bureau). On the other hand, consolidation of support activities and facilities would be appropriate under the regional structure where it is apt to garner efficiencies or cost savings. The Federal Emergency Management Agency (FEMA) should remain an independent agency responsible for coordinating federal response to natural and man-made disasters, including terrorism.
- Enhance the Homeland Security Advisory System. The national alert to state and local governments should be replaced with regional alerts and specific warnings for different types of industries and infrastructure. This will become easier once the Department of Homeland Security completes its comprehensive risk-level ranking of all areas in the country. Hopefully, the ranking will address criteria such as population, threat assessment, number of important sites, and level of vulnerability, and then classify each area as low, medium, or high risk. In addition, DHS must establish capabilities-based performance standards of preparedness and response for state and local authorities. National performance standards will provide a guide to help state and local governments determine what they need to do to counter terrorist threats and what help they should expect from the federal government.

II. Roles and Missions

Border, Immigration, and Transportation Security

Findings. Prior to the creation of DHS, seven agencies (among others) were involved in securing U.S. borders, enforcing immigration laws, and securing the transportation system: the U.S. Customs Service, Immigration and Naturalization Service (INS), Executive Office of Immigration Review, Bureau of Consular Affairs, U.S. Coast Guard, TSA, and Animal and Plant Health Inspection Service (APHIS). Agency missions overlapped to greater or lesser extents, and because the agencies resided in different Cabinet departments, it was difficult to resolve operational and policy conflicts without open turf warfare or resorting to the cumbersome interagency process.

The creation of DHS was supposed to consolidate agencies with overlapping missions and to better integrate our efforts in this area. It has succeeded to some degree. INS has been abolished, and its border inspectors and Border Patrol Agents have been merged with most of U.S. Customs and the border inspectors of APHIS to create U.S. Customs and Border Protection—a single uniformed face at our borders.

However, in “consolidating” responsibility for border, immigration, and transportation security, DHS actually increased the number of involved agencies to eight and created additional problems that now need solving. In addition, it has failed to clearly delineate the missions of DHS agencies that also have border, immigration, or transportation security responsibilities.

Additionally, the split of responsibilities between the CBP and ICE was done without a compelling reason—other than the vague (and ultimately incorrect) descriptive notion that the Customs and Border Protection would handle “border enforcement” and ICE would handle “interior enforcement.” Indeed, in various interviews, not one person has been able to coherently argue why the CBP and ICE were created as separate operational agencies. Indeed, some have compared it to deciding to break up the New York Police Department into two separate agencies—one housing the uniformed “beat cops” (analogous to the CBP’s uniformed officers) and the other housing the detectives (analogous to ICE’s plain-clothes investigators).

Complicating the border security picture is the unclear mission of the TSA. While most Americans associate TSA with baggage screeners at airports, the Aviation and Transportation Security Act that created TSA also makes it responsible “for security in all modes of transportation,” including ensuring the “adequacy of security measures for the transportation of cargo.” This has injected TSA into the realm of border security and created friction with other DHS agencies historically in charge of securing the movement of cargo into the United States—the Coast Guard and CBP. The BTS has not been particularly effective in clearly delineating the relative responsibilities of the CBP and TSA (and it has no authority over the Coast Guard), resulting in policy impasses such as the fights about who is responsible for moving forward on “smart” containers and who is in charge of such programs as Operation Safe Commerce.

Under the Homeland Security Act, responsibility for ensuring that terrorists do not obtain visas to enter the United States is shared by DHS and the State Department’s Bureau of Consular Affairs. This has led to a significant turf struggle. Indeed, the process of negotiating a memorandum of understanding between the State Department and DHS delineating their respective responsibilities took over one year. Additionally, there has been policy paralysis, even as many observers have viewed post-9/11 U.S. visa policy as a disaster—with security trumping all other objectives and deterring many individuals who present no threat from seeking to come to the U.S. or tying them up in excessive bureaucratic delays. The problems associated with post-9/11 visa policy—because of their impact on economic, diplomatic, academic, and scientific exchanges—have the potential to undermine long-term security interests.

Recommendations.

- Rationalize border security and immigration enforcement by merging the CBP and ICE, eliminating the Directorate of Border and Transportation Security. BTS has neither the staff nor the infrastructure to integrate the operations of the CBP and ICE on a consistent basis outside of the occasional task force, such

as the Arizona Border Control Initiative. Nor does it have a policy operation with sufficient influence with the secretary to resolve policy conflicts. Merging the CBP and ICE will bring together under one roof all of the tools of effective border and immigration enforcement—Inspectors, Border Patrol Agents, Special Agents, Detention and Removal Officers, and Intelligence Analysts—and realize the objective of creating a single border and immigration enforcement agency. This reform could be accomplished by executive decision, without the need for legislative action.

- Eliminate the BTS. With the merger of the CBP and ICE into a single agency, there is no need for the BTS middle-management layer. All operational agencies should have a direct reporting relationship to the secretary via the deputy secretary. This will allow for a better, DHS-wide (including the Coast Guard) policy and operational strategic approach to border security matters.
- Consolidate the U.S. Visitor and Immigrant Status Indicator Technology program (US-VISIT) program office into the merged border agency. Currently, the US-VISIT program is run by a stand-alone office in the BTS.
- Refocus and rename the TSA. The TSA should be solely an operational agency with no oversight or infrastructure protection policy functions. The agency should focus on overseeing DHS deployments protecting elements of transportation infrastructure deemed to be of national importance. The most prominent such deployment is currently the TSA screeners at airports, but one could imagine TSA officers deployed to other key transportation nodes if required. Restructuring the TSA's mission would eliminate the policy and regulatory conflicts with CBP and the Coast Guard.
- Responsibility for non-operational transportation infrastructure protection oversight should be in the DHS secretariat. There is no reason to separate transportation infrastructure protection from other types of critical infrastructure protection oversight, state/local/private coordination, and DHS grantmaking.
- Consolidate responsibility for visa operations within a single federal agency. Splitting responsibility for visa issuance and management between DHS and the State Department was a mistake. Operations could be managed more efficiently under one department and would place responsibility and accountability in one place. The choice is difficult. Arguably, the State Department is better positioned to consider the diplomatic, economic, and cultural issues at stake in issuing visas. On the other hand, if DHS were responsible, it would be better able to seamlessly integrate visa management into its other border control responsibilities and coordinate visa operations with its other international responsibilities.

Critical Infrastructure Protection, Preparedness, and Response

Findings. The vast majority of the nation's critical infrastructure is in private, state, or local hands. Likewise, most preparedness efforts are being undertaken by state, local, and private sector entities without federal leadership or control. However, a key and unique DHS mission is leading national—not just federal—efforts to protect critical infrastructure, prepare for possible attacks and other emergencies, and respond to catastrophic incidents such as the 9/11 terrorist attacks.

However, the DHS Secretary's ability to lead is hampered not only by the absence of an Undersecretary for Policy, but also by the fragmentation of key responsibilities among nine entities, both within and outside of DHS:

The DHS Emergency Preparedness and Response Directorate (EPR) is primarily FEMA, but it also includes certain efforts to coordinate with state, local, and private entities in preparing for disasters, including terrorist attacks.

The Infrastructure Protection (IP) piece of the DHS Information Analysis and Infrastructure Protection Directorate (IAIP) identifies critical infrastructure warranting protection, prioritizes efforts, and works with state, local, and private entities to secure this infrastructure. Within the IP sub-directorate is the office in charge of cybersecurity.

The Office of State and Local Government Coordination and Preparedness in DHS is the product of merging the Office of State and Local Coordination and the Office of Domestic Preparedness. It works with state and local governments on identifying needs, coordinating efforts, and doling out DHS grant money for critical infrastructure protection and preparedness.

The Transportation Security Administration. TSA is primarily responsible for aviation security.

The Coast Guard, in addition to its operational responsibilities, is responsible for protecting seaports through risk assessments, reviewing facility security plans, developing Area Maritime Security Plans, coordinating Area Maritime Security Committees, and facilitating Port Security Grants with the Maritime Administration. The Coast Guard also has Strike Teams and Maritime Safety and Security Teams to respond to incidents at ports.

The Office of Private Sector Liaison has primarily been an ombudsman for private efforts to influence DHS policy in various areas, but it conceivably could be a forum for working with the private sector on critical infrastructure protection and preparedness for attacks.

The DHS Science and Technology Directorate Office of WMD Operations and Incident Management is a new office within the Science and Technology Directorate and is intended to provide rapid scientific and technical expertise and decision making in response to weapons of mass destruction (WMD) attacks and incidents.

The Assistant Secretary for Public Health Emergency Preparedness in the Department of Health and Human Services (HHS) and the *Centers for Disease Control and Prevention* also play a part. These agencies outside DHS are central to our ability to prepare for and respond to a bioterrorism attack.

The Department of Energy Nuclear Response Teams provides lead federal response to radiological incidents.

The fragmentation of the U.S. government's leadership efforts into all these discrete—and often competing—agencies has hampered the effort. While we do not recommend transferring outside agencies into DHS given the important interrelationships with their home departments (e.g., the interrelationship between the HHS Assistant Secretary for Public Health Emergency Preparedness with broader public health issues), we do advocate—at a minimum—further consolidations within DHS to unify and focus DHS efforts and to enable the secretary to work effectively with other departments on the critical national priorities of securing critical infrastructure, preparing for terrorist attacks, and responding to them.

Recommendations

- As much as practicable, consolidate DHS response missions into FEMA and strengthen that agency. FEMA should be engaged squarely in its traditional role of planning for the national (not just federal) response to emergencies—including terrorist attacks—and then implementing them where necessary.
- Eliminate the EP&R. Both the proposed Undersecretary for Protection and Preparedness and FEMA should report directly to the secretary via the deputy secretary. As with the BTS, consolidating operational efforts renders the middle-management directorate layer unnecessary. A “flatter” structure is preferable here and will better enable the secretary to exercise leadership. It will be important for the secretary to ensure close coordination between the Undersecretary for Protection and Preparedness and FEMA because the nation’s “preparedness” and “response” efforts are clearly interrelated and require coordinated leadership.

Intelligence Analysis

Findings. The Homeland Security Act created the DHS Intelligence Analysis and Infrastructure Protection Directorate and envisioned that it would serve as the nation’s mechanism for fusing all foreign and domestic intelligence relating to potential terrorist threats against the homeland, consolidating all of the disparate terrorist and law enforcement watchlists, and generally “connecting the dots” needed to prevent another attack—correcting a problem seen as contributing to the 9/11 tragedy.

However, this role has not developed as envisioned by the act. Instead, after a significant period of bureaucratic competition among the DHS, CIA, and FBI, the President established the Terrorist Threat Integration Center (TTIC) to perform the task of “connecting the dots” and facilitating the sharing of intelligence among federal agencies under the direction of the Director of Central Intelligence with the DHS and FBI serving as deputy directors. In a subsequent executive order, Homeland Security Presidential Directive 6, the President created the Terrorist Screening Center (TSC) and established it as a mechanism for consolidating the watchlists. The TSC is also an interagency activity, but it operates under the FBI with DHS serving in a deputy role.

By creating the TTIC and TSC, the President diminished the importance of the IAIP's intelligence fusion role. The DHS Assistant Secretary for Information Analysis now plays a much less significant role than originally envisioned by Congress. His current roles are: (1) serving as the DHS Secretary's intelligence advisor; (2) coordinating the intelligence and information analysis components within DHS, including those resident in the agencies; (3) serving as DHS's voice to the intelligence community, including the TTIC and TSC; and (4) ensuring that the TTIC and TSC are adequately staffed with DHS personnel. DHS also has a significant operational role in analyzing information to determine targets for greater scrutiny. Indeed, this is the key mission of the National Targeting Center (NTC), which is currently run by U.S. Customs and Border Protection and which works closely with the IAIP, TTIC, and TSC.

The National Commission on Terrorist Attacks Upon the United States (the "9/11 Commission") recommended the creation of a National Counterterrorism Center (NCTC), which would serve under a National Intelligence Director and be responsible for coordinating all domestic and foreign counterterrorism operations. Legislation proposed by the U.S. House and Senate calls for implementing this measure and placing the TTIC within the NCTC. This initiative may serve to further marginalize the intelligence integration function of DHS and its capacity to represent the terrorism intelligence "consumer" community, including its subordinate agencies and a host of state, local, and private sector entities.

Recommendations. DHS should have a chief intelligence officer whose responsibilities include: (1) acting as the secretary's principal intelligence advisor and providing integrated analysis for the department and wider homeland security community; (2) disseminating and incorporating intelligence into other DHS components; (3) receiving, integrating, and disseminating intelligence and threat warnings to the private sector and state and local governments; and (4) representing the secretary to the intelligence community.

Placement of the TTIC should be carefully considered. There is a strong consensus that the nation requires a greater capacity to share and compare intelligence regarding terrorism. Clearly, the TTIC has a critical role to play in accomplishing this task. For the TTIC to accomplish this mission it must have both the authority of the President and the ability to tap the resources of all federal agencies. In addition, it must be able to draw on information and expertise from state and local governments and the private sector and equitably serve the needs of all these constituents. These factors need to be weighed carefully in deciding whether the nation would be better served by having the TTIC (while remaining an interagency activity) report to the DHS Secretary and work closely with the TSC, the NTC, and ICE's Law Enforcement Support Center or by making the TTIC part of the NCTC supporting global operations against terrorism.

At its core, the TTIC's mission should be: (1) analyzing domestic and foreign intelligence and law enforcement information to identify potential threats to the homeland; (2) communicating that information to law enforcement and other prevention agencies (many of which are housed in the DHS); and (3) warning the public. There may be other missions envisioned—and these activities are vital to supporting the missions of other agencies—but they are all also central to DHS's intended mission.

III. Authorities

Department Oversight

Findings. Congress has not consolidated oversight of DHS's homeland security functions into single committees in the House and Senate. The final report of the 9/11 Commission reaffirmed the importance of fixing congressional oversight. The commission held that:

Congress should create a single, principal point of oversight and review for homeland security. Congressional leaders are best able to judge what committee should have jurisdiction over this department [DHS] and its duties. But we believe Congress has the obligation to choose one in the House and one in the Senate, and that this committee should be a permanent standing committee with a nonpartisan staff.

As the report also noted, one expert witness appearing before the commission testified that the lack of effective congressional oversight is perhaps the single greatest obstacle impeding the successful development of DHS.

The creation of various oversight offices within DHS, including a Privacy Office and an Office for Civil Rights and Civil Liberties, is a positive step. However, the functions of DHS, and their coordination and interaction with other homeland security and national security entities, require a more robust and less conventional oversight function than currently exists. Oversight and transparency lend credibility to the exercise of homeland security authorities and instill confidence in the American people. Conversely, without strong oversight, even well-intended initiatives and programs may be weakened or discontinued out of suspicion, ignorance, and lack of credibility with the public. This is especially the case with intelligence collection, intelligence analysis, and information sharing initiatives and activities for homeland security.

Recommendations.

- Create a more robust oversight structure for homeland security, beginning with an effective, rationalized, and consolidated oversight and authorization committee structure in Congress and an enhanced recommitment to intelligence oversight on the part of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Oversight should not only protect against abuse, but should also ensure efficiency and effective interagency processes in areas such as information sharing and technology development.
- Inculcate a culture of self-oversight through best management practices, with regular training for line officers on regulations and limitations of authority, utilizing lessons learned and best practices from agencies that have a long, successful history of legal compliance, such as the National Security Agency.

The chief focus of oversight should be to conduct regular audits and periodic reviews of ongoing activities, rather than after-the-fact investigations. As the nation builds the substantive homeland security regime, we must also develop a worthy oversight regime, clarifying oversight mechanisms and determining the appropriate mix of congressional, judicial, administrative, and inspector general oversight.

Specialized offices such as civil liberties boards and privacy officers ought to be reviewed for effectiveness and redundancy. Overseers must review and seek improvements not only in the internal functioning of DHS and other agencies, but also in their interaction with each other—particularly in information sharing, areas of joint or overlapping responsibility, and dealing with unstructured, fluid situations such as cyberattacks and bio-attacks.

Information Sharing and Technology Development and Acquisition

Findings. There exists an intricate, distributed, but necessary web linking the flow of information from intelligence collection and aggregation to analysis and, ultimately, to sharing with appropriate policymakers and security officials. This web is built upon, and sustained by, a mosaic of enabling technology that is integrated into a network

to enhance information sharing. The homeland security community has a fragmented and inadequate process to ensure that technological innovations develop alongside the changes in policy, privacy protection, and oversight that are made necessary by these technological innovations. This gap between technology and appropriate policy structures leads to missed opportunities in homeland security technologies, because promising new technologies are not pursued as aggressively as they might be out of concern for their impact on privacy and civil liberties.

DHS lacks adequate authorities and mechanisms to clarify how the development of controversial new technologies and the development of democratic controls over their use should proceed side by side. The department is missing the capacity to evaluate the intrusive effects of data mining and data aggregation and how they can be mitigated by privacy protection (e.g., anonymization and judicially managed access to identities), guidelines and standards, oversight, and technology to reduce the risk of abuse (e.g., immutable audit trails and strong access and authentication controls). The department also lacks the capacity to efficiently issue appropriate guidelines to ensure that technologies are used appropriately.

It is critical to move forward with developing capabilities and mechanisms for information sharing. This development must proceed hand-in-hand with crafting policy guidelines for information sharing. For example, technology development should be informed by clear policy about necessary predicates for and restrictions on access to sensitive information, controls on retention and dissemination, and requirements for authentication and auditing. Other critical policy questions include determining how private sector information can be accessed and used. DHS should have clear legislative mandates to address these issues.

Recommendations. The federal government must create a process to couple innovations in technology with innovations in law, so that we neither deny ourselves opportunities in homeland security technologies nor erode civil liberties and economic progress. This process must work across all research and development agencies and operational agencies of the government and involve the appropriate congressional overseers.

DHS needs to serve as the lead advocate for funding promising technologies for homeland security and for the development of these technologies in ways consistent with the requirements of civil liberties, privacy protection, and economic efficiency. As new technologies are funded and developed, DHS needs to take the lead—in advisory committees or in insertion of ongoing and milestone legal and policy reviews within technology programs—in identifying, evaluating, and addressing head-on the potential policy and legal problems of technologies. DHS should also work with other agencies, Congress, and appropriate outside experts to provide guidance on how best to prototype, test, and implement these technologies in tandem with the safeguards and standards that should accompany their use.

Protection of Sensitive, but Unclassified Information

Findings. Improving information sharing is critical, but here it is necessary to strike the right balances in sharing information with or withholding information from the public. Policies that are either overly neglectful or overzealous ill serve efforts to enhance homeland security. For example, the discovery on al-Qaeda hard drives of information on critical infrastructure vulnerabilities, bomb making, and other potentially dangerous information downloaded from open websites caused the U.S. government to rethink its policies on information published on government websites. Some agencies responded by withdrawing virtually all information from their public websites. Others have seriously curtailed the amount of useful information or public access to unclassified information that is available from sources other than their websites. At the very least, such wholesale withdrawal of information seems arbitrary and undermines important values of government openness, the development of electronic government (e-gov) to speed the delivery and lower the cost of government services, and public trust.

The Homeland Security Act contained a requirement for regulation of Protected Critical Infrastructure Information (PCII). That regulation was finalized in spring 2004, and DHS now has a PCII office. This effort addresses only some areas of sensitive information. It is not sufficiently comprehensive.

The process for classifying secret information in the federal government is disciplined and explicit. The same cannot be said for unclassified but security-relevant information for which there is no usable definition, no common understanding about how to control it, no agreement on what significance it has for U.S. national security, and no means for adjudicating concerns regarding appropriate levels of protection. To date, there has been no systematic

review of what government information that is now or was formerly in the public domain could be used as a “terrorist roadmap,” the likelihood of such a threat, the role that such information would play in terrorists’ preparation (including possibilities of alternative sources of the same information), and the countervailing public safety and other benefits of providing different types of information. Furthermore, no authority is clearly designated to make these evaluations at a national policy level. Current evaluations are conducted at the departmental level at best or on an ad hoc, office-by-office basis. Nor has DHS provided any leadership or guidance to the private sector about how the private sector might develop voluntary standards for making decisions about its own disclosures of sensitive information, even without governmental restrictions. For government decisions, there is no single designated authority—in the Office of Management and Budget or elsewhere—for determining the overall policy interests and objectives of information distribution, including common baseline standards to help weigh the benefits and risks of providing the public with specific types of information, regardless of which agencies possess the information. Such a single authority might act as the overall reviewer of agencies’ public disclosure policies and their implementation of these policies.

Recommendation. There must be consistent policy and legislation that encourages the sharing of unclassified but security-relevant information between the private sector and the government. This policy must be sensitive to the public benefit of openness and should not unnecessarily remove information from public access. A clear and balanced policy on disclosure would also address private sector fears of business losses due to public disclosure of proprietary information (e.g., through error, court documents, and public security announcements), of liability for disclosure, and of private citizens’ fears of inappropriate and overreaching government secrecy.

Clarification of Authorities for Critical Missions

Findings. DHS is an amalgamation of several new and previously existing entities, each with its own organic authorities and regulations. Seams and overlaps in roles, missions, and authorities still exist. Some agencies have overlapping missions, while other missions remain unassigned or unclaimed by specific agencies. Three areas are of particular concern: (1) cyberattack, (2) incidents and attacks involving biological agents and toxins, and (3) activities within the intelligence community.

It is not apparent that DHS has sufficient authorities to meet its assigned responsibilities under the National Strategy to Secure Cyberspace. Nor is it clear who would be in charge of the response to a cyberattack on the United States, what kind of response would be legally authorized, and what authorities would be required in different scenarios of detection, verification/validation, attribution, response, and reconstitution or recovery. It is also not apparent what process would be followed to coordinate investigative steps and responses among agencies and to assign roles and authorities as factual information about the attack emerges. Elements of the National Infrastructure Protection Center transitioned to DHS. At the FBI, these watch, warning, and training elements worked closely with law enforcement agents. At DHS, the role of these elements in a cyberattack is uncertain. The Secret Service, which investigates computer fraud and computer-based attacks on the financial system, is another important element of DHS’s cyber-related capabilities.

It is also unclear which agency would have primary responsibility for responding to a biological attack on the United States, which DHS office would lead its operational bio-response (whatever that would be), and whether federal agencies would support or take the lead in supporting a state or local response to a bio-attack. In part, this confusion results from the fact that the agencies with the primary legal authorities and expertise in bio-defense—such as the Department of Health and Human Services (Public Health Service, Centers for Disease Control, National Institutes of Health, and Office of the Secretary of HHS), the Department of Agriculture, and DOD—have responsibilities that transcend homeland security (e.g., public health, epidemiology, and national defense). Thus, the authorities for bio-defense response are neither well-coordinated nor harmonized.

DHS’s legal authorities and responsibilities as a member of the intelligence community are unclear. For example, it appears that the department has sufficient authority to accomplish effective information sharing. However, it needs new authorities for a career intelligence service and in support of counterintelligence operations, as well as new dissemination guidelines. Lack of clarity also permeates the roles and missions of DHS within the intelligence community, both as a producer of intelligence and as a consumer of intelligence.

Recommendations. Authorities and national leadership roles for bio-defense, cyberdefense, and critical infrastructure protection need to be clarified by establishing and empowering lead federal executives. The issue of DHS authorities to prepare and respond to cyberattacks requires additional discussion. Clarification of the department's role, in turn, should be reflected in future changes in the roles, missions, and management of the department. Currently, it is unclear which federal agency should lead the response to a cyberattack, given that there are many capabilities for detection and response throughout several federal agencies, including the DHS, Department of Justice, DOD, and intelligence community, as well as in the private sector.

In general, greater consolidation of authorities for bio-defense and medical responses to catastrophic terrorism would likely result in a more efficient and coordinated federal response. Where possible, authorities over national medical response programs such as the Metropolitan Medical Response System and the National Disaster Medical System should be harmonized and coordinated under DHS direction with substantial input from HHS, which has greater expertise and experience in these issues as well as long-standing relations with relevant stakeholders.

The DHS intelligence entity must have well-defined authorities and the legal instruments to accomplish its missions in the intelligence community. These missions include not only DHS as a consumer of intelligence, but also as a disseminator of intelligence to federal, state, and local authorities.

Congress and the executive branch need to make a significant effort to reconcile the information sharing needs of DHS with existing law on sharing information (e.g., the Privacy Act, the USA PATRIOT Act, and classification rules).

Watchlists, Profiling, and Policies for Information Protection

Findings. Although the Homeland Security Act and Homeland Security Presidential Directives 6 and 11 provide clear guidance for managing watchlists, there is inadequate guidance and effort in establishing standards for profiling, composition and consolidation of terrorist watchlists, avenues of recourse for persons who wish to challenge their placement on a watchlist, and review of the government's use of watchlists. First, in view of the significance of terrorist watchlists and the harm to an innocent individual who is erroneously placed on such a list, there is a necessity for government-wide guidance on constructing these lists comprehensively and accurately. Second, there is also a compelling need for an appropriately transparent procedure by which an individual who alleges that he or she has been erroneously placed on the list may contest and overturn the listing. At the same time such a procedure must be sufficiently rigorous and discerning that it prevents efforts by terrorists to remove themselves from watchlists.

In addition, there is insufficient clarity about when and how profiling (singling out certain persons for heightened scrutiny or other actions) is authorized and appropriate. Issues that have not been adequately addressed include: What are the necessary authorities to support profiling? When can profiling be employed? What actions (e.g., further investigation or detention) can be justified by profiling? What standards and safeguards should accompany profiling? Should standards and safeguards differ depending on the mission and potential negative consequences of profiling? For example, should a higher standard be applied to using a profile to prohibit someone from boarding a commercial aircraft in the United States than to conducting a traffic stop to question truck drivers near a sensitive location? If profiling is used, how should it be informed by data mining and other information analysis techniques in addition to watchlists?

Recommendations. The federal government should accelerate its efforts to consolidate and police its watchlists. DHS should take the lead in implementing processes, enforced by authorities, to develop comprehensive and accurate watchlists. This must include authorities and processes to correct errors, configuration control to enhance utility and interoperability of information across agencies, and regular review and oversight. Laws or regulations should be developed specifying standards of proof, limitations on what information related to watchlists can be given to the individual of concern, and requirements to correct errors as they are adjudicated.

As part of the effort to enhance the integrity and value of watchlists, an adjudication process needs to be established with a neutral third-party decision maker operating with defined rules and standards—perhaps an administrative law judge—to oversee the review of lists and adjudicate claims brought by individuals who assert that they were erroneously placed on a watchlist. Similarly, DHS should take the lead in formulating standards for determining what kinds of heightened scrutiny or investigation are appropriate when an individual on a watchlist is identified.

IV. Resources

Authorization Process

Findings. The efficient use of federal resources requires an effective partnership between the executive and legislative branches. Although departments receive daily operational guidance from the executive, Congress has the constitutional responsibility to fund these departments and oversee their operations to achieve efficiency and accountability. Currently, Congress has not responded coherently to the challenge of overseeing DHS's allocation and use of resources. Even though separate appropriation subcommittees have been formed, there is no established process to authorize expenditures.

An authorization bill for DHS could serve as a critical statutory management tool by providing a means to exercise stronger oversight of important DHS activities, such as key personnel programs, performance of critical missions, major research programs, and information technology investments. In July 2004, the House Select Homeland Security Committee unsuccessfully attempted to markup a DHS authorization act.

Congress should reconsider the reauthorization process for the full scope of critical national security programs. Under current law, Congress must pass a Department of Defense authorization bill every year. Historically, this has been appropriate because national security was focused solely on defeating America's enemies overseas. However, 9/11 made it abundantly clear that security at home is equally vital. The magnitude of these dual challenges underscores the need for Congress to pay equal attention to both missions. Homeland security is simply too important to be pushed to the legislative sidelines for years at a time. On the other hand, given the numerous "must pass" bills that Congress already faces each year, requiring passage of an annual DHS authorization bill might be too much.

Recommendations. Congress should legislate a Department of Homeland Security Authorization as envisioned by the House Select Homeland Security Committee. Establishing permanent homeland security committees in both the House and Senate with full jurisdiction over DHS would greatly facilitate this effort.

Congress should consider reauthorizing homeland security and defense spending biannually: Each Congress could pass a DOD authorization bill in one session and a DHS authorization bill in the other. Considering the demands facing Congress, biannual authorization bills would be a realistic approach to focusing lawmakers' attention and balancing oversight of DHS and DOD. Biannual bills would provide greater opportunity for the two departments to implement new congressional directives effectively while allowing Congress more time to evaluate how well the respective departments are implementing statutory guidance. They could also bring additional legislative stability and predictability to annual appropriations for the two departments.

Allocation of Grants

Findings. One of the great strengths of American democracy is the dispersion of power at every level of governance with the goal of allowing local citizens to have the most say in local decisions. Preservation of the principles of federalism must remain a key goal in creating an effective and sustainable homeland security regime. That means that each level of government and the private sector must fulfill its responsibilities.

The federal responsibility of providing financial resources to state and local governments remains a contentious issue. The first and highest priority for federal spending must be investments that assist in creating a true national preparedness system. Federal funding should focus on programs that will make all Americans safer. That includes providing state and local governments with the capability to integrate their counterterrorism, preparedness, and response efforts into a national system and expanding their capacity to coordinate support, share resources, and exchange and exploit information. The federal government must also help to build the capacity to respond to catastrophic terrorism—acts of violence so terrible and destructive that they exceed the ability of any state or local government to respond effectively.

However, there are no federal criteria for the minimum capabilities needed to protect an American community, no funding formula that is based on risk analysis and divorced from politics, and no funding system that can assure a sustained flow of funds for specified projects that are consistent with the real security needs of the community and national strategic priorities. Additionally, there is no legislative requirement for federal grants to be allocated in a manner that supports the national homeland security strategy.

As the 9/11 Commission reported, the current grantmaking process is in danger of becoming pork-barrel legislation. Allocation of most homeland security grants is established by a congressionally mandated formula. Current funding formulas guarantee each state 0.75 percent of the funds available. As a result, 40 percent of funds are immediately tied up, leaving only 60 percent for discretionary allocations. In this manner, in 2003, California received only 7.95 percent of general grant monies, even though the state accounts for 12 percent of the nation's population. Wyoming, which received 0.85 percent, accounts for only 0.17 percent of the population. This translates to \$5.03 per capita in California and \$37.94 per capita in Wyoming. Within states, rural, less populated areas often receive a disproportionate amount of money as well. Some states distribute funds equally among counties, resulting in amounts that are so small that it is difficult to imagine how they could be used productively. Even the Urban Area Security Initiative grants, monies targeted at major population areas that are also considered potential targets, produce curious results. Under the current formula, San Francisco (with a population of 800,000) and Los Angeles (with a population of 4 million) receive about the same amount of money.

Recommendations. The Department of Homeland Security should continue to implement Homeland Security Presidential Directive 8, which requires DHS to take the lead in rationalizing the funding of homeland security priorities and establishing a set of minimum essential capabilities for every American community so that state, local, and federal governments can work together to achieve these standards. Establishing national performance standards for preparedness is essential to evaluating readiness, determining priorities, and targeting investments.

Congress should establish risk-based funding formulas for port security, emergency responder, and other non-federal grants that are consistent with the national homeland security strategy. For example, Congress could adopt the proposal in the Cox-Turner bill (Faster and Smarter Funding for First Responders Act, H.R. 3266) that guarantees states only 0.25 percent of funding rather than the current 0.75 percent and assigns the rest of the funds on a risk-based system. Title V of the 9/11 Recommendations Implementation Act (H.R. 10) contained a similar provision.

National Threat/Vulnerability Assessments

Findings. In the three years since the September 11 attacks, our nation has created the third largest bureaucracy in the federal government and spent close to \$100 billion on efforts to secure the homeland from further terrorist attack. Yet we still have not completed a threat/vulnerability assessment that can help to develop strategy, set priorities, and guide spending in a targeted, sustainable manner for what will certainly prove to be a long-term conflict against terrorism.

With only limited resources available to achieve the almost limitless goal of protecting the entire United States against terrorist attack, it is critical that we set priorities. These priorities should be based on a comprehensive threat/vulnerability matrix that identifies which areas need the most protection and have the greatest urgency.

Many officials have recognized the need for such an assessment, and it has been promised for years. The latest DHS estimate is that such a study will be completed by 2008, but America cannot wait that long.

Recommendation. The Department of Homeland Security must assume strong leadership of this project and deliver a comprehensive threat/vulnerability assessment to America's top national security decision makers by December of 2006. It should be based on commonly accepted risk-assessment methodology. Spending and missions conducted by DHS could then be logically prioritized based on what is most vital to protect the nation.

Response to Catastrophic Terrorism

Findings. America is not sufficiently prepared to respond fully to a catastrophic terrorist attack on U.S. soil that involves chemical, biological, radiological, or nuclear (CBRN) weapons.

The 9/11 attacks made clear that the number of Americans our terrorist enemies seek to kill is limited only by the power of their weapons and not by the darkness of their imaginations. Current response capabilities for such an attack are scattered across the spectrum of state, federal, and local governments. For example, the U.S. military has some capability to respond in environments contaminated by a CBRN attack. However, these units are primarily trained for maintaining their missions in a battlefield environment rather than restoring order and providing relief in a major American city. Various state National Guards maintain Civil Support Teams, which are being trained for deployment in such hot zones, but the teams are new and are not able to respond nationally. The federal government maintains strategic stockpiles of vaccines at several locations, but the recent shortage of flu vaccine, the inability to mobilize rapidly and efficiently to deliver scarce vaccines to high-risk individuals, and the long gear-up timetable to meet the objectives of Project Bioshield should be causes for concern.

Protecting America from and responding to potential terrorist attacks that utilize weapons of mass destruction is clearly constitutionally mandated by the phrase "provide for the common defense." Only the federal government has the power, personnel, and resources to prepare and organize the massive response that would be needed to respond to the casualties and recover from a WMD attack on U.S. soil. The federal government must provide the means to scale the national response to meet terrorist threats up to—and including—catastrophic attacks.

Recommendations. Based on national risk assessments and a national survey of the capacity and readiness of assets across the country to respond to catastrophic terrorism, DHS should develop contingency plans that include national "response packages," allocations of resources that including regional (e.g., multi-state) and federal entities that would be available to respond to various types of emergencies, from natural to manmade. These response packages should be scalable, in sufficiently modular means so that they can be efficiently deployed to a range of disasters. If DHS determines that these response packages are inadequate, it should explore the feasibility of establishing a Homeland Security strategic reserve that will assemble additional response capabilities.

Border Security

Findings. The 9/11 Commission rightly singled out border security and terrorist travel as subjects of grave concern. Indeed, these represent a complex problem for protecting America at home. However, the challenges of border security are more than just securing the border. They cut across issues of foreign policy, economic development, immigration, internal enforcement, trade, maritime commerce, air travel, rail and ground transport, and border control. On land, at sea, and in the air, providing resources to meet U.S. security needs is a daunting task.

On land, over 1 million non-U.S. citizens illegally cross the U.S. border each year, circumventing U.S. immigration law and identity screening procedures. On the southern border alone, over 20,000 "other than Mexican" people from "countries of interest" (e.g., Pakistan, Iran, and Afghanistan) are detained each year for illegally crossing the U.S. border. Historically, they have been released if they promise to return for a hearing at a future date, but almost all disappear without a trace due to a lack of facilities and personnel.

At sea, the U.S. Coast Guard has been given additional roles in the wake of 9/11. The Coast Guard now must assess port security at hundreds of U.S. ports, monitor the voyages of thousands of foreign-flagged vessels into U.S. ports, and provide rapid response and boarding capability in case of potential danger. As the lead agency responsible for the security of America's shores and waterways, the Coast Guard has a tremendous new responsibility in the 21st century—however, its personnel levels and fleet have not dramatically changed in a generation.

In the air, security is best assured through the diligent and effective efforts of TSA screeners on the ground and air marshals on board passenger aircraft. However, the level of TSA screeners has dropped substantially, from 60,000 to 45,000, with no apparent reason provided for the drop except the will of appropriators on congressional committees.

Recommendation. DHS must conduct a national assessment of the resources required for effective border security, including all the layers of security that impact securing the border. This analysis should be used to help Congress and the Administration determine where to direct resources to ensure that funding is directed toward programs that provide the greatest contribution to supporting the critical border security mission

Task Force Participants

Task Force Co-Chairmen

James Jay Carafano
 Senior Research Fellow for Defense and Homeland Security
 Kathryn and Shelby Cullom Davis Institute for International Studies
 The Heritage Foundation

David Heyman
 Director and Senior Fellow, Homeland Security Program
 Center for Strategic and International Studies

Participants

Scott Bates
 Senior Policy Adviser
 Select Committee on Homeland Security
 U.S. House of Representatives

Christian Beckner
 Fellow, Homeland Security Program
 Center for Strategic and International Studies

Jonah Czerwinski
 Director of Homeland Security Projects and Senior Research Associate
 Center for the Study of the Presidency

James Dean
 Deputy Director, Government Relations
 The Heritage Foundation

Mary DeRosa
 Senior Fellow, Technology and Public Policy Program
 Center for Strategic and International Studies

Gerald L. Epstein
 Senior Fellow, Science and Security
 Homeland Security Program
 Center for Strategic and International Studies

Jay Farrar
 Vice President for External Affairs
 Center for Strategic and International Studies

Brian Finch
 Associate
 McKenna Long and Aldridge, LLP

Reagan Fuller
 Manager, Federal Government Relations
 French and Company

Task Force Participants

DHS 2.0

Daniel Kaniewski
 Deputy Director
 Homeland Security Policy Institute
 The George Washington University

Alane Kochems
 Homeland Security Research Assistant
 Kathryn and Shelby Cullom Davis Institute for International Studies
 The Heritage Foundation

Ronald D. Lee
 Partner
 Arnold & Porter LLP

Terry Maynard
 Independent Consultant

Lillian McTernan
 Program Coordinator, Homeland Security Program
 Center for Strategic and International Studies

Steve Metruck
 Military Fellow, International Security Program
 Center for Strategic and International Studies

Keith Miller
 Research Assistant
 Thomas A. Roe Institute for Economic Policy Studies
 The Heritage Foundation

Ha Nguyen
 John F. Kennedy School of Government
 Harvard University

Kate Phillips
 Research Associate, Homeland Security Program
 Center for Strategic and International Studies

Neal A. Pollard
 General Counsel
 Terrorism Research Center, Inc.

Daniel Prieto
 Research Director, Homeland Security Partnership Initiative
 Harvard University

Rebekah Robblee
 Kathryn and Shelby Cullom Davis Institute for International Studies
 The Heritage Foundation

Paul Rosenzweig
 Senior Legal Research Fellow
 Center for Legal and Judicial Studies
 The Heritage Foundation

David Schanzer
 Select Committee on Homeland Security
 U.S. House of Representatives

Seth M.M. Stodder
Senior Counsel
Akin Gump Strauss Hauer & Feld, LLP

Virginia Thomas
Director, Executive Branch Relations
The Heritage Foundation

Irvin Varkonyi
President
Supply Chain Operations Preparedness Education, LLP

Richard Weitz
Senior Staff Member
Institute for Foreign Policy Analysis

Anne Witkowsky
Senior Fellow, Technology and Public Policy
Center for Strategic and International Studies

Evaluating the Security of
the Global Containerized
Supply Chain

Henry H. Willis, David S. Ortiz

Approved for public release, distribution unlimited



RAND INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

The research described in this report results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

Library of Congress Cataloging-in-Publication Data

Willis, Henry H.
Evaluating the security of the global containerized supply chain / Henry H. Willis, David S. Ortiz.
 p. cm.
 "TR-214."
 Includes bibliographical references.
 ISBN 0-8330-3715-3 (pbk. : alk. paper)
 1. Shipping—Security measures. 2. Unitized cargo systems—Safety measures. 3. Container ports—Security measures—United States. 4. Marine terminals—Security measures—United States. 5. Terrorism—United States—Prevention. I. Ortiz, David (David Santana) II. Title.
 HE735 W55 2004
 363.32—dc22
 2004024937

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2004 RAND Corporation

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2004 by the RAND Corporation
 1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
 1200 South Hayes Street, Arlington, VA 22202-5050
 201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
 RAND URL: <http://www.rand.org/>
 To order RAND documents or to obtain additional information, contact
 Distribution Services: Telephone: (310) 451-7002;
 Fax: (310) 451-6915; Email: order@rand.org

Preface

A global supply chain links the United States and its economy to the rest of the world. The unit of measure of the supply chain is the shipping container: a sturdy steel box of standard dimensions that carries most freight. Millions of containers circle the earth on specialized ships, railcars, and trucks. Actions to ensure the security of the system of containers and their conveyances have traditionally focused on preventing smuggling and theft. Since September 11, 2001, supply-chain security has been redefined as preventing terrorists from targeting the containerized supply chain or transporting a weapon in a shipping container. The change in focus raises questions about the effectiveness of proposed security efforts and the consequences they may have for supply-chain efficiency.

This report outlines a framework for assessing and managing supply-chain security and efficiency. It identifies key stakeholders in the system, defines critical capabilities of the supply chain, and reviews current efforts to improve supply-chain security and efficiency. This framework also defines a path for future research and is to be the first of a series of studies on the topic of supply-chain security. The results of this study will be of interest to public and private decisionmakers responsible for policies and investments to manage components of the supply chain.

This report results from the RAND Corporation's continuing program of self-initiated research. Support for such research is provided, in part, by donors and by the independent research and development provisions of RAND's contracts for the operation of its U.S. Department of Defense federally funded research and development centers.

Contents

Preface	iii
Figures and Tables	vii
Summary	ix
Abbreviations	xv
SECTION 1	
Motivation and Introduction: Toward a Model for Assessing Supply Chain Security	1
SECTION 2	
Proposed and Implemented Security Measures Since September 11, 2001	4
Customs-Trade Partnership Against Terrorism	4
Operation Safe Commerce	4
The Container Security Initiative	4
The Maritime Transportation Security Act of 2002	5
Antitamper Seals	5
Radio-Frequency Identification	5
X-Ray and Gamma-Ray Scanning	5
Radiation Pagers, Portal Sensors, and Remote Monitoring	6
SECTION 3	
The Global Supply Chain: Points of View, System Components, and Stakeholders	7
The Transaction Layer: A Business Fulfillment Network	8
The Logistics Layer: A Multimodal Physical Network for the Transport of Cargo	10
The Oversight Layer: The Legal and Regulatory Structure of the Global Supply Chain	12
Interactions Among Layers in the Supply Chain	13
SECTION 4	
Capabilities of the Global Container Supply Chain	16
SECTION 5	
Managing Container Shipping Security: A Case of Technology-Induced Risk	18
Building Supply-Chain Capabilities	18
Customs-Trade Partnership Against Terrorism: Making Supply-Chain Participants	
Responsible for the Security of Container Cargo	19
Operation Safe Commerce: Harnessing Technology to Improve Customs Inspection	
Effectiveness	19

Container Security Initiative: Increasing Deterrence and Efficiency Through Cargo	
Inspection at Foreign Ports	21
Maritime Transportation Security Act: Reducing Theft and Improving Incident Response	
at Ports and on Vessels.....	21
Antitamper Seals: Improving the Integrity of Container Shipping	21
Radio Frequency Identification: Improving the Transparency of Supply-Chain Networks	22
X-Ray and Gamma-Ray Scanning: Improving Transparency of Cargo Shipments.....	22
Radiation Pagers, Portal Sensors, and Remote Monitoring: Increasing Capabilities to Detect	
Weapons of Mass Destruction	22
 SECTION 6	
Preliminary Conclusions, Recommendations, and Future Inquiry	23
Preliminary Conclusions	23
The Inseparability of Supply-Chain Security and Efficiency.....	23
Potential Underinvestment in Fault Tolerance and Resilience	25
Recommendations	26
The Public Sector Should Seek to Bolster the Fault Tolerance and Resilience of	
the Logistical Supply Chain.....	26
Security Efforts Should Address Vulnerabilities Along Supply-Chain Network Edges	26
R&D Should Target New Technologies for Low-Cost, High-Volume Remote	
Sensing and Scanning	26
Future Inquiry	27
References	29

Figures and Tables

Figures

S.1. Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain	x
1. The Business Transaction Network	9
2. The Supply Chain Seen in Terms of People and Places	11
3. Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain	14

Tables

S.1. Organizational Interests	x
S.2. Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events	xii
1. Organizational Interests	14
2. Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events	20

Summary

The global supply chain is the network of suppliers, manufacturing centers, warehouses, distribution centers, and retail outlets that transforms raw materials into finished products and delivers them to consumers (Simchi-Levi, Kaminsky, and Simchi-Levi, 2002). Security of the system has traditionally focused on reducing shrinkage—the loss of cargo shipments through theft and misrouting. However, heightened awareness of terrorism has redefined supply-chain security—the consequences of an attack on or via a critical global port could be a tremendous loss of life and a crippling of the U.S. economy—and has brought increased attention to the risks containerized shipping presents.

The response has been proliferation of new security measures. For all these efforts, is the system of trade more or less secure? Will we know if these efforts are successful? How will success or failure be measured? This report presents a strategy for answering these questions using methods for managing risk of large-scale systems to analyze the structure of the container supply chain and its properties.

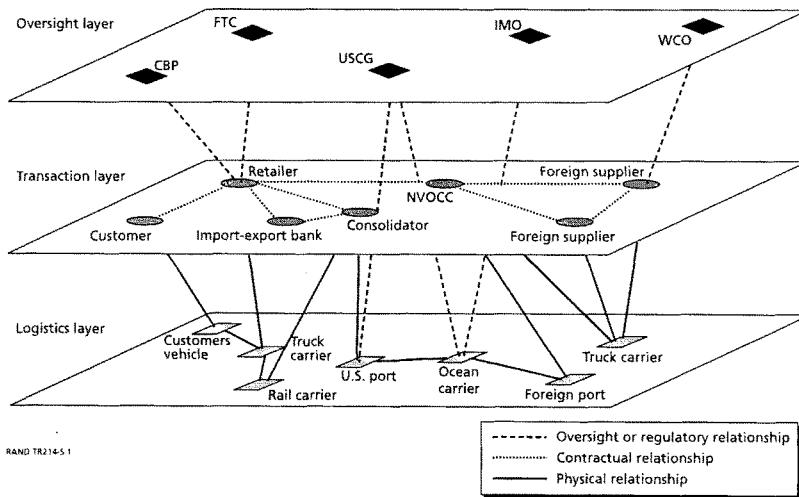
The Three Layers of the Global Container Supply Chain

The structure of the global container supply chain would seem self-evident: It is a system of vessels, port facilities, railcars, trucks, and containers that transport goods in discrete units around the earth. That view, however, pertains only to the physical components of a system that includes the cargo, information, and financial flows required for the system to operate. We propose viewing the supply chain as three interdependent and interacting networks: a physical logistics system for transporting goods; a transaction-based system that procures and distributes goods and that is driven primarily by information flows; and an oversight system that implements and enforces rules of behavior within and among the subsystems through standards, fines, and duties. Network components are *nodes*, such as factories and ports, and *edges*, such as roads and information links. Figure S.1 illustrates the subsystems as a collection of layers. The oversight system has agencies and organizations that interact with the layers of the global container supply chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The *logistics layer* is responsible for the movement of cargo along a network of roads; the *transaction layer* orders goods and materials from a network of suppliers; and the *regulatory layer* specifies standards for operation within its area of authority.

Table S.1 lists examples of the organizations present in each layer. The three layers may be specified by the organizations that comprise each. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Figure S.1

Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The logistics layer is responsible for the movement of cargo along a network of roads; the transaction layer orders goods and materials from a network of suppliers; and the regulatory layer specifies standards for operation within its area of authority.

**Table S.1**

Organizational Interests. The three layers may be specified by the organizations that comprise each layer. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Layer	Examples of Stakeholders	Examples of Oversight Agencies
Transaction	Wal-Mart Target Ford Non-Vessel-Operating Common Carriers (NVOCCs)	Federal Trade Commission U.S. Customs and Border Protection World Customs Organization
Logistics layer	International Longshore and Warehouse Union Pacific Maritime Association International Labor Organization CSX Transportation APL Maersk Sealand Port of Long Beach	U.S. Department of Labor U.S. Department of Homeland Security Local law enforcement U.S. Coast Guard U.S. Customs and Border Protection World Customs Organization

Examining the supply chain from each of these perspectives yields insights into the concerns of relevant stakeholders, the levers available to improve supply-chain performance, and the interactions among the layers that improve or detract from system performance.

Capabilities of the Global Container Supply Chain

The ability of the global container supply chain to deliver goods efficiently and securely can be described through five measurable capabilities:

- **Efficiency.** Container shipping has evolved primarily to deliver goods more quickly and more cheaply than other modes of transport, when volume and mass are taken into account.
- **Shipment reliability.** Supply chains must behave as expected, retrieving and delivering goods as directed, with a minimum amount of loss due to theft and accident.
- **Shipment transparency.** The goods that flow through a supply chain must be legitimately represented to authorities and must be legal to transport.
- **Fault tolerance.** The container shipping system should be able to respond to disruptions and failures of isolated components without bringing the entire system to a grinding halt.
- **Resilience.** A supply chain is resilient insofar as it is able to return to normal operating conditions quickly after the failure of one or more components. Resilience is a function of both the system's design and the responsiveness of the oversight layer.

The efficiency of the container shipping system is measured in terms of its speed and cost, taking reliability into account. Security, however, is a function of the final four capabilities. Efficiency and security are often portrayed as in direct conflict, but in our formulation, they are measured differently and may support or hinder one another, depending on the circumstances. Analysis of any program's efficiency and security implications needs to consider the system under both normal and emergency operating conditions.

Managing Risk in the Global Container Supply Chain

We applied a framework of technology-induced risk assessment (Morgan, 1981) to provide insight into how supply-chain security capabilities are realized. Table S.2 details how policy and technology proposals support improved supply-chain capabilities. This table presents the perspective of capabilities that could be captured by private shippers, carriers, and port operators and by the U.S. government. Through application of this methodology, we also get a high-level view of how these objectives come together as an integrated container security strategy. The methodology also reveals gaps in the set of policies intended to improve the security of the global container supply chain: fault tolerance and resilience, for instance, have received little attention from policymakers.

Table S.2
Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events

Policy or Technology	Driving Layer	Anticipated Supply Chain Efficiency Effects	Anticipated Supply Chain Security Effects		
			Threat or Vulnerability Reduction	Reduce Probability of Attack	Mitigate or Compensate for Consequences
Customs-trade partnership against terrorism	Transaction and logistics	Reduced shipping cost and time and increased volume; <i>Expedited customs</i>	Reduced fraud: <i>Detect at entry</i>		
Operation Safe Commerce	Logistics and oversight		Reduced damage and fraud: <i>Detect at origin</i>		
Container security initiative	Oversight		Reduced theft: <i>Control access</i>		Increased Fault tolerance and resilience: <i>Disaster planning</i>
Maritime Transportation Security Act of 2002	Oversight				
Anti-tamper seals	Transaction and logistics		Reduced damage: <i>Detect at origin</i> Reduced fraud: <i>Detect at origin</i>		
Radio frequency identification	Transaction and logistics	Reduced shipping cost and time: <i>Improved Logistics</i>	Reduced damage, losses, and fraud: <i>Deter terrorists, thieves, and smugglers</i>	Reduced theft losses: <i>Detect unapproved transport</i>	Increased resilience: <i>Rapid location and rerouting of shipments following a disaster</i>
X-ray and gamma-ray inspection	Logistics and oversight		Reduced damage: <i>Detect at origin</i> Reduced fraud: <i>Detect at entry</i>		
Radiation pagers, portal sensors, and remote monitoring	Logistics and oversight		Reduced damage: <i>Detect at origin</i>	Reduced damage: <i>Detection before cargo enters ports</i>	

Preliminary Conclusions

Applying the layered capabilities framework to the analysis of current efforts to improve supply-chain security led us to two conclusions:

- **Supply-chain efficiency and security are distinct but interconnected.** Efforts to improve the efficiency of the container shipping system may or may not have affected the security of the system. In turn, security efforts might also improve efficiency. Those that do not may lead to unexpected negative consequences as the system adapts to compensate for or work around resulting losses of efficiency.
- **Both public- and private-sector initiatives to improve the security of the global supply chain have focused largely on preventing and deterring smuggling and terrorist attacks.** These initiatives focus on improving the transparency of the global container supply chain. Few initiatives have focused on improving the fault tolerance or resilience of the system, which could be a fruitful area for new security measures.

Recommendations

These conclusions suggest three complementary paths for improving the security of the global container supply chain while maintaining its efficiency:

- **The public sector should seek to bolster the fault tolerance and resilience of the global container supply chain.** The closure of a major port—for whatever reason—would have a significant effect on the U.S. economy. The federal government should lead the coordination and planning for such events for two reasons. First, the motivation of the private sector to allocate resources to such efforts is subject to the market failures of providing public goods. Second, the government will be responsible for assessing security and for decisions to close and reopen ports.
- **Security efforts should address vulnerabilities along supply-chain network edges.** Efforts to improve the security of the container shipping system continue to be focused on ports and facilities (although many ports around the world still failed to meet International Ship and Port Security Code guidelines even after the July 1, 2004, deadline.) Unfortunately, the route over which cargo travels is vast and difficult to secure. Measures to keep cargo secure while it is en route are essential to a comprehensive strategy to secure the global container supply chain.
- **Research and development should target new technologies for low-cost, high-volume remote sensing and scanning.** Current sensor technologies to detect weapons or illegal shipments are expensive and typically impose significant delays on the logistics system. New detection technologies for remote scanning of explosives and radiation would provide valuable capabilities to improve the security of the container shipping system.

Future Inquiry

This report is our initial assessment of the security of the global container supply chain; our work is continuing in the following areas:

1. assessment of policies for improving supply-chain security
2. systems analysis of supply-chain risk
3. technology assessment and research and development planning for improving supply-chain performance
4. economic analysis of global trade trends on supply-chain performance.

Abbreviations

BE	bill of exchange
CBP	U.S. Customs and Border Protection
CIS	U.S. Citizenship and Immigration Services
CSI	Container Security Initiative
CSX	CSX Transportation
C-TPAT	Customs-Trade Partnership Against Terrorism
FTC	Federal Trade Commission
GAO	General Accounting Office
IB	import bank
IMO	International Maritime Organization
MTSA	Maritime Transportation Security Act
NVOCC	Non-Vessel-Operating Common Carrier
OECD	Organisation for Economic Co-Operation and Development
OSC	Operation Safe Commerce
POLB	Port of Long Beach
RFID	radio frequency identification
SB	seller's bank
TAPA	Technology Asset Protection Association
TSA	Transportation Security Administration
USCG	U.S. Coast Guard
WCO	World Customs Organization

SECTION 1

Motivation and Introduction: Toward a Model for Assessing Supply Chain Security

The global supply chain is an international system that has evolved to make the transport of freight throughout the world amazingly efficient. The chain consists of the suppliers, manufacturing centers, warehouses, distribution centers, and retail outlets that move raw materials, work-in-progress inventory, and finished products from producer to consumer (Simchi-Levi, Kaminsky, and Simchi-Levi, 2002). The shipping container and its transport system are integral components of the global supply chain.

Approximately 90 percent of the world's cargo is shipped via container, including 75 percent (by value) of non-North American trade to and from the United States (Stana, 2004). There are approximately 18 million containers of various sizes around the world. The standard container is a 20-ft equivalent unit, which is a sturdy steel box measuring 20 × 8 × 8 ft, although containers are often 40 ft long and can come in various configurations to support different kinds of cargo (Pollack, 2004). These containers are bolted to the chassis of trucks, stacked two high on flatbed railcars, and packed onto ships as large as aircraft carriers carrying thousands of such containers. Port operations and technology are optimized so that ships spend a minimum amount of time at the quay and the maximum time en route.

The principal concern of business is to increase the efficiency of the global supply chain, paying comparatively little attention to security. In recent years, ocean carriers have cut crews to an absolute minimum and have continued to order larger and faster ships in an effort to squeeze every cent of profit from the system (Pollack, 2004).

Prior to September 11, 2001, supply-chain security focused primarily on reducing shrinkage—the loss of cargo shipments through theft and misrouting. This risk motivated action in the private sector. In 1997, 60 high-technology companies collaborated in the Technology Asset Protection Association (TAPA) (Flynn, 2000). These firms are consumer electronics and computer manufacturers and retailers, for whom theft represents a considerable business risk. TAPA developed and issued guidelines for shipping security for these products, and “if a freight forwarder or carrier wants to do business with any of TAPA’s well-heeled members, they must adopt these practices” (Flynn, 2000). TAPA now includes European members, and it issues security requirements and self-evaluation tools to potential service providers.¹

The problems of theft and smuggling demonstrate the relative ease with which criminal elements have capitalized on the use of containers as conveyances. Anonymity of contents, opaque ownership arrangements for vessels, and corruption in foreign ports have all facilitated the efforts of those who are inclined to use container shipping for illegal purposes.

¹ Documentation is available on TAPA’s Web site (TAPA, 2004).

More recently, the private sector has looked to new technologies for solutions for improving supply-chain efficiency and reducing shrinkage. Wal-Mart, for example, has mandated that its suppliers use radio-frequency identification (RFID) tags to increase the visibility of the shipping and purchasing process and to improve the efficiency of the supply chain; in the case of drug shipments, it is also hoped that the tags will help combat counterfeiting (Feder, 2004). The Smart and Secure Tradelanes Initiative consortium applies RFID technology at the container level, and in its initial report, it notes that current supply-chain processes are engineered for efficiency, productivity, and flexibility, with minimal emphasis on security. To the extent that security is a consideration, it is focused on reducing cargo theft and protecting proprietary data from competition (Smart and Secure Tradelanes, 2003).

Heightened awareness of terrorism has redefined supply-chain security and increased attention to the risks containerized shipping presents. The west-coast port lockout of 2002 suggested the magnitude of economic effects a terrorist-related event might cause. Estimates placed the losses for the ten-day lockout between \$4.7 billion and 19.4 billion (Iritany and Dickerson, 2002; Cohen, 2002).

Steven Flynn of the Council on Foreign Relations has been among the most vocal proponents of heightening the security of the international supply chain. He writes that a terrorist organization could easily ship people, arms, or even a weapon of mass destruction in a standard cargo container (Flynn, 2004). Given that over 7 million containers enter the United States every year through its seaports and that few of these containers are physically inspected, the containerized shipping system seems to present an attractive target (GAO, 2003).² The magnitude of the system and its unparalleled passion for efficiency at all levels support Flynn's hypothesis. Security experts believe it is only a matter of time before the United States or one of its allies is the victim of a terrorist attack using a shipping container, resulting in significant loss of life and in widespread and global economic damage.

Since September 11, 2001, emphasis on port and maritime security has increased. The International Maritime Organization (IMO) has updated the International Ship and Port Security code to require port, carrier, and vessel security plans and personnel. The United States has responded with parallel legislation in the form of the Maritime Transportation Security Act of 2002 (MTSA), which requires similar actions for U.S. ports and vessels and appoints the U.S. Coast Guard (USCG) as the organization responsible for compliance and enforcement. The World Customs Organization, the World Shipping Council, the Pacific Maritime Association, the United Nations Council on Trade and Development, U.S. Customs and Border Protection (CBP), the Transportation Security Administration (TSA), and every one of the 361 U.S. ports and most international ports have all initiated responses.

The urgency of these responses is justified by the gravity of the potential for loss of life if terrorists were able to use the container shipping system successfully. However, for all these security efforts, is the system of trade more secure? How insecure was it in the first place? Will we know if these efforts are successful? How will success or failure be measured?

The costs and scale of security measures to counter this threat demand analysis of what other effects such attacks might have and how the security measures themselves affect performance of the container shipping system. This report presents a framework for answering these questions.

² Some U.S.-bound containers arrive at Canadian ports, entering the United States via truck or rail.

Our discussion is organized as follows. Section 2 describes security measures that have been implemented or proposed since September 11, 2001. Section 3 depicts three perspectives on the supply chain: (1) a logistics network of roads, tracks, and sea-lanes that moves cargo from an origin to a destination; (2) a transaction network linking buyers, sellers, and their financial intermediaries; and (3) an oversight system regulating operation of the logistics and transaction networks to protect public safety and levy tariffs. These perspectives represent three interconnected layers of networks and identify stakeholders in different stages of the supply chain. They also illustrate the levers available for realizing improved supply-chain security and efficiency. Section 4 defines the capabilities of a secure and efficient supply chain.

Building on these descriptions of the containerized shipping system, Section 5 lays out a framework for assessing and managing supply-chain security. Drawing from literature on technology-induced risk, we examine current security approaches and policies from the perspective of how they affect supply-chain capabilities and which stakeholders they involve. Finally, we close with a discussion of insights that this risk assessment framework provides about current port security efforts and future directions for research to support policymaking to protect U.S. ports, trade lanes, and the container supply chain.

Our focus is on U.S. domestic policies for the operation of ports and maritime vessels as nodes in the global container supply chain; we have limited ourselves to this subset of the global container supply chain because it has been the subject of the majority of proposed measures for protecting the security of containerized shipping in the face of the terrorist threat. Future analysis will address the system in general, including its global nature and the security issues related to intermodal transport.

SECTION 2

Proposed and Implemented Security Measures Since September 11, 2001

The response to the terrorist threat to container shipping has been multifaceted. It has involved evaluation and adoption of new technologies, passage of new regulations, and implementation of new operating processes and protocols. To date, most efforts have concentrated on maritime shipping operations (as opposed to intermodal transport). The focus on seaports has occurred for two principal reasons: Seaports are America's principal connections to the global economy, and seaports are bottlenecks in the system at which it is possible to impose additional security provisions. This section presents an overview of some major U.S. and international initiatives and technologies to improve supply-chain and port security taken since September 11, 2001. We will refer to these initiatives as we develop our analytical framework.

Customs-Trade Partnership Against Terrorism

The goal of Customs-Trade Partnership Against Terrorism (C-TPAT) is to push responsibility for cargo security onto stakeholders in the supply chain. C-TPAT is a voluntary program that shippers and carriers can enter to assure CBP that they have put into place the best security practices for the packing, tracking, and distribution of all containers and goods en route to the United States. In return, shippers and carriers are rewarded through quicker processing and reduced probability of inspection delays (CBP, 2004).

Operation Safe Commerce

Operation Safe Commerce (OSC) is a technology-development and -deployment program intended to improve the ability of customs agents to detect illicit cargo on its entry into a port. According to TSA (2004), "OSC is a collaborative effort between the federal government, business interests, and the maritime industry to develop and share best practices for the safe and expeditious movement of containerized cargo." Through a set of grants, OSC is promoting the testing, evaluation, and fielding of container scanning and tracking technologies.

The Container Security Initiative

The Container Security Initiative (CSI) inspects and clears containerized cargo before shipment to the United States (CBP, undated). Through this program, CBP has deployed

inspectors at 19 of the world's major seaports in Europe, Asia, Africa, and North America. The goal of CSI is to make it more difficult to transport illegal shipments to the United States by implementing inspections at ports of origin, thus increasing U.S. security. Although CBP has offered to station foreign customs inspectors at U.S. ports, none have accepted to date.

The Maritime Transportation Security Act of 2002

MTSA dictates that domestic ports and carriers with U.S.-flagged vessels develop and institute port, port area, and vessel security plans and register these plans with the USCG (MTSA, 2002). These requirements establish standards and protocols for port security, inspections, and emergency response. MTSA is the U.S. version of the IMO's International Ship and Port Security Code (IMO, 2004).

Antitamper Seals

Antitamper seals are a broad set of technologies that detect and indicate when an unauthorized party has opened a container. They range from electronic devices that record when and by whom containers are opened to proposals to mark containers with unique "fingerprints" that are modified when a container is opened or compromised. Even the simplest antitamper seals, such as high-quality cable seals, are considerably more expensive than common bolt seals.

Radio-Frequency Identification

RFID technologies allow shippers and carriers to track cargo while it is within the container shipping system. The devices can record and transmit information about a container's origin, destination, contents, or processing history. RFID systems are typically designed to transmit information about cargo when the shipment passes salient portals, such as entry or exit from a port or when the cargo is loaded or unloaded from a ship.

RFID devices are available as both passive and active technologies. Passive devices transmit only when in the presence of a reader that provides the required power. They have ranges up to a few meters and are typically used to track shipments at the unit or carton level. Active devices are battery powered and can transmit over distances as far as 100 m or more. Thus, active devices have been applied to tracking cargo at the container and pallet levels.³

X-Ray and Gamma-Ray Scanning

X-ray and gamma ray technologies are used to scan containers for misrepresented or illegal shipments. These technologies allow CBP to visualize for nonintrusive inspections of a con-

³ Bear-Stearns has issued several analyses of RFID technology and solutions providers (Alling, Wolfe, and Brown, 2004; Wolfe et al., 2003).

tainer' contents, obviating the need to open it and inspect the contents physically. Currently, between 5 and 6 percent of containers are inspected either intrusively or nonintrusively (Wasem et al., 2004). Application has been limited because of the cost of the machines, the lack of space at ports, the time required to scan, and the relatively high false-positive rates that result from the inconclusive visualizations that the technologies provide (Stana, 2004).

Radiation Pagers, Portal Sensors, and Remote Monitoring

Technologies for the remote sensing of weapons of mass destruction are under development. Radiation pagers are portable devices that can be used to detect nuclear or radiological weapons as inspectors move throughout a port or vessel. Portal sensors are designed to detect weapons of mass destruction as containers enter and leave ports or vessels. These and other remote-monitoring devices to detect weapons of mass destruction and other illegal cargo are in early development. However, capabilities are expected to improve over time and possibly be integrated with RFID or other container tracking technologies.

SECTION 3

The Global Supply Chain: Points of View, System Components, and Stakeholders

Section 1 discussed the global supply chain generally as the system of containers and conveyances in which and on which goods flow from producers to consumers. This view is too coarse to permit a formal analysis of the properties of the supply chain. In fact, there are several ways in which to characterize the system, each with unique properties and performance measures.

To a product-based business, the supply chain is its network of suppliers and sub-suppliers. This *transaction layer* connects participants to each other legally through contracts, informationally through product specifications, financially through transaction records, and physically through the actual product or good.

The delivery system, the *logistics layer*, is a conveyance through which products move. The system of roads, tracks, and sea-lanes and the containers that flow along them comprise a network, one that provides services to the producers and consumers of goods. Members of the business community would prefer that the physical system be transparent; that a financial transaction plus an associated waiting time be all that is required to guarantee the movement of products, the particular truck, train, or boat not being of consequence (World Shipping Council, 2003).

An *oversight layer*, consisting of customs organizations, law enforcement, and national and international bodies, oversees the contracting for and movement of goods. At times, the oversight bodies work within a particular layer of the supply chain: USCG guarantees maritime safety and security, and the Federal Trade Commission (FTC) monitors the actions of firms to ensure compliance with trade law. At other times, the organization must interact with both layers: CBP is responsible for the collection of duties and for helping to ensure port security.

The transaction, logistics, and oversight layers of the supply chain each form a network.⁴ For example, in the logistics layer, the *nodes* are all facilities through which the cargo

⁴ The flow of goods on networks is a mature topic in logistics (Ford and Fulkerson, 1962). More recently, researchers have studied the structure and dynamics of social, physical, and transportation networks (Watts, 1999; Holmes, 2004). An edge in a social network may be represented by a business relationship between two firms: Goodyear supplies tires to General Motors, for example. Two properties of networks concern us in this study: the small-world phenomenon and the property of "connectedness." A *small world* is a network that has relatively few edges leading to and from the average node but that has a small number of successive edges that connect any two nodes. The most famous example is the notion that there are "six degrees of separation" between any two humans (Guare, 1990). Small-world phenomena have been demonstrated in the electric power grid, the Internet, and in the nervous systems of animals (Watts, 1999). Intuitively, one would think that the nodes with the most edges are responsible for reducing the number of "jumps," but this is not the case: It is the nodes that connect two so-called well-connected nodes that guarantee the small-world phenomenon (Watts, 1999). *Connectedness* is the property of a network that all nodes are connected to all other nodes through a set (or sets) of edges. These properties together govern the resilience of the system. Amaral et al. (2000) studied several types of small-world networks and showed that certain types of networks are able to better maintain connectedness in the face of attacks on nodes and edges than are

travels from origin to destination, and the *edges* (i.e., the links that connect nodes) are the roads, railroad tracks, and sea-lanes on which the cargo moves. Examination of the supply chain from each of these perspectives yields important insights into both the concerns of relevant stakeholders and the levers available to improve supply-chain performance.

The Transaction Layer: A Business Fulfillment Network

For a company, the supply chain is the collection of individuals or firms that supply material for the production or sales of a product. The supply chain for a cookie manufacturer would, at a minimum, include suppliers of butter, flour, sugar, flavorings, and packaging. These suppliers are held to performance standards for their products and for delivering them subsequent to an order: The butter must have a certain percentage of milk fat; when an order is placed, the supplier is expected to fill the order and deliver the butter within a specified time. The cookie manufacturer should have little concern for the particular route that the butter took from its supplier, only that it arrived within a prespecified window of time.⁵ The relationships between the manufacturer and its suppliers are based on legal contracts for the fulfillment of orders.

This transaction-based view of the global supply chain can be represented as the union of two interacting networks: an information network and a material network. The information network coordinates the flow of goods and payments and is regulated by U.S. and international trade law. The material network for a particular firm includes all direct and indirect suppliers of goods. Failures of nodes in the transaction layer are fundamentally different from failures in the logistics layer described in the next section.

The transaction layer views the logistics layer as a conveyance mechanism. A failure in the transaction layer eliminates the source of a product or the financial flows that trigger logistics demands; a failure in the logistical system limits the flow of goods through a particular port, rail yard, or truck stop or along a particular route. For example, a disruption to a supplier of polo shirts—a node in Wal-Mart's supply chain—is fundamentally different from a disruption to a seaport—a node in the logistics layer. The disruption to the garment factory affects its suppliers and customers, but a disruption to a port affects all cargo that would have passed through it, polo shirts and automobiles alike, with far greater economic consequences. Figure 1 illustrates the contracting and payment mechanism among the seller, the seller's bank, the import bank, and the buyer for a bill of exchange for goods (Organization for Economic Cooperation and Development [OECD], 2003), the goods pass through the logistics layer, represented as a gray bar in the center of the figure.

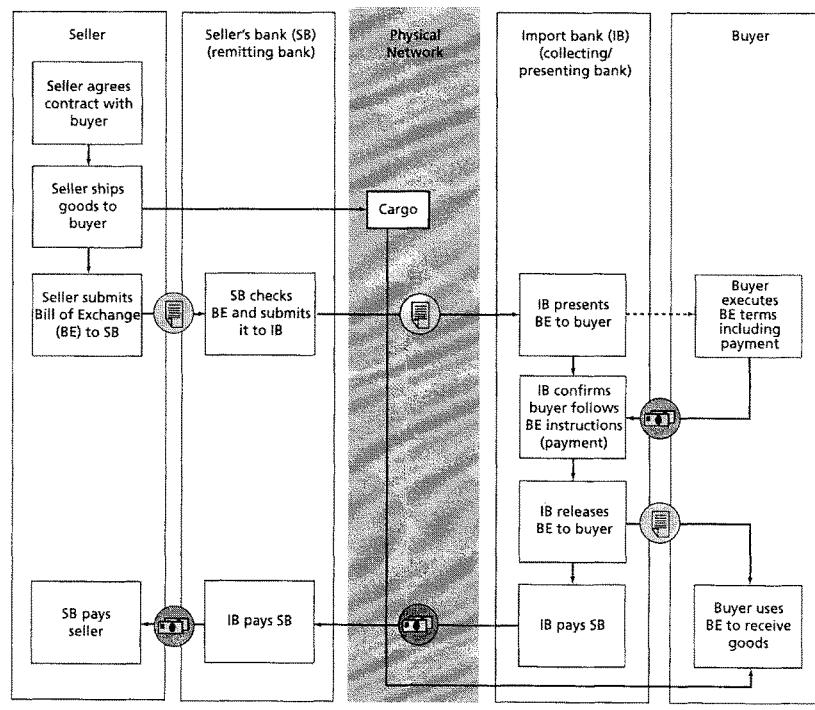
The business layer has been used to improve supply-chain performance in several ways. First, companies searching for a competitive advantage have become early adopters of technologies and policies to improve supply-chain security and efficiency. The Smart and Secure Tradelanes Initiative is one such example: A consortium of technology vendors, shippers, and port operators is evaluating technologies and processes to increase network transparency to reap the presumed security and efficiency benefits (OECD, 2003).

others. We will appeal to network-theoretic notions throughout this work, but we will not directly assess the network properties of the international supply chain in this analysis.

⁵ This is not always the case: Wal-Mart monitors all costs diligently and recently rerouted Chinese cargo from Hong Kong to Guangdong to save \$650,000 annually on shipping (Cleeland, Irriany, and Marshall, 2003).

Figure 1

The Business Transaction Network. The transaction that results in the shipments of goods from a seller to a buyer and the exchange of funds between the buyer and seller sees the logistic network as a conveyance for products. This illustrates the contracting and payment mechanism among the seller, the seller's bank, the import bank and the buyer for a bill of exchange for goods.



SOURCE: OECD, "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee report, 2003. Online at <http://www.oecd.org/home/> (as of November 5, 2003). Adapted and used with permission.

Second, organizations with market power have used the business layer to demand improved supply-chain security. For example, Wal-Mart and the Department of Defense have demanded that their largest suppliers use RFID at the carton and unit level to track shipments.

Third, companies that ship high-value goods, for which there are established gray and black markets, are also demanding improved security. Examples include Hewlett-Packard for computers, Intel for chips, and Pfizer for pharmaceuticals (Sheridan 2004).

Also, C-TPAT enlists shippers and retailers, with specialized security recommendations for the business supply chain (CBP, 2004).

The Logistics Layer: A Multimodal Physical Network for the Transport of Cargo

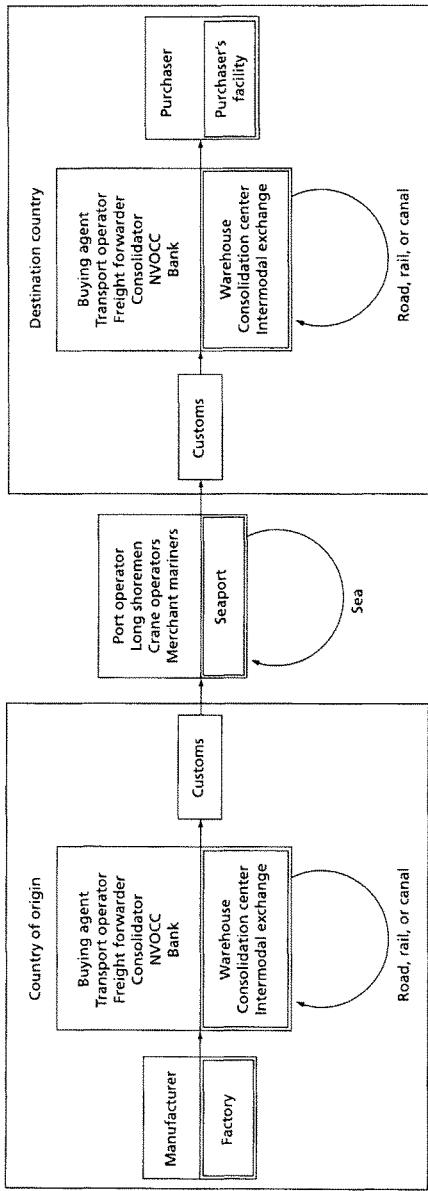
The supply chain can also be viewed as the physical system on which goods travel. This point of view is shared by those who operate the supply chain as a business: trucking companies, rail freight firms, ocean carriers, the International Labor Organization and the International Longshore and Warehouse Union, freight forwarders and consolidators, etc. This view of the supply chain merges two perspectives illustrated in a report written for OECD. In OECD (2003), author Philippe Crist considered the supply chain from the points of view of the places through which cargo travels and of the people who have access to cargo at various stages. These two perspectives are better considered together, since cargo does not move autonomously. Figure 2 consolidates two figures from OECD (2003), illustrating the movement of cargo in terms of the persons who have access to it (single-lined boxes) and by the places to which it travels (double-lined boxes and arrows). Actions to secure the supply chain follow these figures by limiting the access of people to the cargo or by securing the routes and conveyances on which it travels.

Merging the two figures allowed us to build on Crist's analysis. In particular, we should understand that the system comprises many self-similar layers: Participants fundamentally perform the function of receiving goods from one carrier and passing them along to the next; each is both a "customer" and a "supplier" (Nishiguchi and Beaudet, 2000). Therefore, the linear progression illustrated in Figure 2 is more accurately viewed as a web of directed connections among producers and consumers. Within each transport mode, there is a network of paths and nodes through which goods can travel. A shipment from a supplier to a consumer may take a number of different paths, with the paths dependent on such factors as the weather and potential security obstacles. The figure depicts these varied paths as feedback loops.

Failure of the shipping network may have more drastic consequences than it would for other infrastructure networks. Fundamental differences affect the applicability of recent results in network theory to the roadway, rail, and port terminal networks that form the global supply chain. In social, information, and certain physical networks, the flow over the network is instantaneous or nearly so. If an Internet router fails, packets are rapidly redirected along an alternative path, avoiding the fault. Some networks are able to operate despite the loss of many nodes (Amaral et al., 2000). But if a port should be closed because of a terrorist attack or, more commonly, because of an accident or spill, rerouting land and sea traffic to avoid the disruption carries significant delays and costs. For perishable food items, for example, delays can result in total loss of cargo value. Further analysis is required to determine the costs of rerouting container traffic around failed nodes and edges.

The majority of initiatives designed to increase the security of the global supply chain have focused on securing the nodes of the network, particularly seaports. A typical seaport capable of handling container traffic will service or house most of the relevant stakeholders, including the CBP, the USCG, freight forwarders and customs brokers, and ocean carriers, and will have links to the rail and highway networks. Unfortunately, seaports are also hubs, in which the road, rail, and sea networks have a common connection. MTSA (2002) and the International Ship and Port Security code of IMO focus their initiatives on measures to improve port security (OECD, 2003). These measures include the designation of an officer

Figure 2
The Logistics Layer in Terms of the Systems and People that Move Cargo. This figure combines two figures from OECD (2003), illustrating the movement of cargo in terms of the persons who have access to it (single-lined boxes) and by the places to which it travels (double-lined boxes and arrows). Actions to secure the supply chain follow these figures by limiting the access of people to the cargo or by securing the routes and conveyances on which it travels.



RAO/TRA/2
 SOURCE: OECD, "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee report, 2003. Online at <http://www.oecd.org/home/> (as of November 5, 2003). Adapted and used with permission.

responsible for port security and the design and approval of a port security plan. Port access controls and worker identification and background checks are also required: Mariners who wish to disembark at a U.S. port must hold a D-1 visa including a biometric identifier (Lloyd's List, 2004), and TSA is developing an identification card for all transportation workers (TSA, 2004).

Other initiatives seek to guarantee the security of containers en route. MTSAs and the International Ship and Port Security code also specify the designation of vessel security officers and vessel security plans in hopes of maintaining the container's security as it travels along an edge of the network. CSI stations CBP personnel in foreign ports to facilitate the approval of U.S.-bound containers, on the assumption that the edge—the sea-lane between the foreign port and the U.S. port—is secure. The C-TPAT initiative enlists carriers in promoting security among partners, including conveyance security, access controls, procedural security, and manifest security (CBP, 2004). Although voluntary, C-TPAT seeks to ensure the security of the edges of the network by enlisting the help of those who have possession of a container as it travels between nodes. C-TPAT has been criticized both for its procedures (Stana, 2004) and for the lack of resources provided for implementation (Flynn, 2004). The transportation network forming the edges of the logistics layer spans the earth, and ensuring the security of containers via direct oversight is impossible in practical terms.

Finally, new technologies may improve security in the logistics layer. Electronic seals are used to detect tampering after the containers have been filled. Active RFID technology projects transparency on the supply chain to allow tracking containers from origin to destination. X-ray and gamma-ray scanning devices allow detection of smuggling of illegal or misrepresented cargo. Remote sensors help inspectors identify hazardous cargo or weapons. Certain government programs, such as OSC, seek to speed the development and deployment of new technology to increase supply-chain security. The Smart and Secure Tradelanes initiative is a private-sector program demonstrating the effectiveness of the new technologies.

The Oversight Layer: The Legal and Regulatory Structure of the Global Supply Chain

Each transaction or movement of goods over the supply chain occurs under the auspices of a regulatory regime consisting of all the rules, regulations, and enforcement mechanisms that govern the structure and operation of the transaction and the physical layers of the supply chain. The focus of these regulations has recently shifted from safety and trade facilitation to security. Current initiatives, such as the International Ship and Port Security code and MTSAs, focus on increasing access restrictions to ports and vessels and on implementing security plans based on a particular threat level. The regulatory and oversight bodies at a U.S. port include the USCG, the CBP, the U.S. Citizenship and Immigration services, and local law enforcement and emergency response agencies. The business network linking sellers to buyers has its own governing legal and regulatory structure. The import and export regulations established by U.S. trade law are enforced by the Department of the Treasury and the FTC. Banks monitor transactions and extend lines of credit to firms. A body of contract and labor law governs the production and procurement of goods. Each piece of regulatory apparatus collects information to ensure that its directives are being met, and these data together form the intelligence that allows targeting of shipments.

In the aftermath of the terrorist attacks of September 11, 2001, new regulation has focused almost exclusively on security measures. The focus on security is a dramatic shift from the previous regulatory regime, which focused on reducing fraud and smuggling, while ensuring the safety of participants in the supply chain, reducing the environmental consequences of trade (e.g., oil spills and air pollution), and collecting all relevant tariffs and duties. We do not know whether these measures have led to the neglect of previous regulatory and enforcement goals, such as the detection and seizure of illegal drugs. Furthermore, terrorism can be prevented using many of the same means used for preventing theft and smuggling because each objective requires that the system be able to control what cargo enters and leaves the system.

New security measures focus primarily on port terminals, although some provisions extend to the high seas. MTSA and its international counterpart, the International Ship and Port Security code, require port security assessments and plans, as well as vessel security plans. But the ocean mode of the system represents only a single vulnerability. Vessel security procedures are intended to protect the integrity of cargo while it is between ports and out of view, but the ocean is also one of the areas in which the ability to compromise cargo is limited to terrorist groups with considerable resources and training.

Even with increased attention on port and maritime components of container shipping, vulnerabilities remain. In the United States, the majority of containers travel to their ultimate destinations by tractor-trailer over the interstate highway system. Along this system, the ability to track an individual shipment is limited; since the highway system is open to the public, the shipment is far more vulnerable. Along the highway network, the regulatory structure is much more diffuse, and local law enforcement must concern itself primarily with public safety. Rail systems are less accessible than the highway system but suffer from similar vulnerabilities and have arguably less oversight.

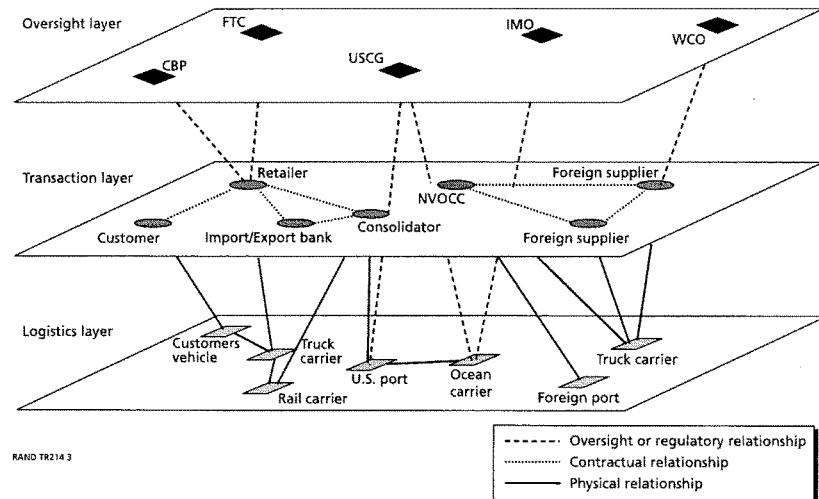
Interactions Among Layers in the Supply Chain

The three points of view each form a layer of the supply chain, each of which depends on the others; we begin with the transaction layer. In the transaction layer, the movement of raw materials, work-in-progress inventory, or finished goods represents the fulfillment of an order. Figure 3 depicts a retailer, who contracts with a foreign supplier and a common carrier to deliver the goods. The carriers in the logistics layer move freight across sea, rail, and road networks. Interacting with the other layers is the oversight layer, which sets the rules under which the lower layers operate. The regulatory network specifies actions that should be taken to secure the supply chain, levies fines, and sets standards. Note that the oversight functions are diffuse: The national and regulatory agencies evolved with specific industries but are now called on to ensure security of the supply chain. For example, U.S. Customs and Border Protection is responsible for enforcing U.S. trade law in addition to ensuring the security of the containerized supply chain.

Table 1 lists some of the organizations that comprise the transaction and logistics layers and the relevant oversight bodies. Note that oversight agencies have limited influence over organizations in either the transaction or the logistics layer.

Figure 3

Interactions Between the Logistics, Transaction, and Oversight Layers of the Supply Chain. The different points of view of the supply chain can be viewed in terms of a layered set of networks. The logistics layer is responsible for the movement of cargo along a network of roads; the transaction layer orders goods and materials from a network of suppliers; and the regulatory layer specifies standards for operation within its area of authority.

**Table 1**

Organizational Interests. The three layers may be specified by the organizations that comprise each layer. Note that oversight agencies have a limited range of influence over organizations in either the transaction or logistics layer.

Layer	Examples of Stakeholders	Examples of Oversight Agencies
Transaction	Wal-Mart Target Ford Non-Vessel-Operating Common Carriers (NVOCCs)	Federal Trade Commission U.S. Customs and Border Protection World Customs Organization
Logistics Layer	International Longshore and Warehouse Union Pacific Maritime Association International Labor Organization CSX Transportation APL Maersk Sealand Port of Long Beach	U.S. Department of Labor U.S. Department of Homeland Security Local law enforcement U.S. Coast Guard U.S. Customs and Border Protection World Customs Organization

Figure 3 and Table 1 also give us a method for assessing the interests of the large number of stakeholders in the system. Any organization involved in the physical movement of cargo is part of the logistics layer. The organizations responsible for staffing and operating the system that moves cargo are also part of the logistics layer. Therefore, all ocean carriers, rail freight providers, trucking companies, port operators, and their vendors (shipyards, crane works, etc.) are stakeholders in the logistics layer. The personnel and carriers are intertwined

such that the actions of one have a direct and measurable effect on the other. This is not the case for the transaction layer, for whose business the participants in the logistics layer compete—it is, after all, the freight of the Wal-Mart, Target, Home Depot, Dell Computer, Ford Motors, and others that the supply chain moves.

The layered model allows a clean demarcation of the lines of responsibility for securing the international supply chain. For example, the C-TPAT program encourages supply-chain participants to make the effort to guarantee the security of cargo and persons under its control.⁶ It also obliges participants to communicate guidelines for security to supply-chain participants with whom it interacts. Companies that participate in C-TPAT receive a favorable reduction in their cargo's risk score when entering U.S. ports (United Nations Conference on Trade and Development Secretariat, 2003).

The layers in the figure illustrate domains of influence for communicating guidelines. Firms involved in the physical movement of freight are able to communicate guidelines to other physical movers most effectively, while large retailers or importers are able to communicate most effectively with their suppliers on issues of security. The C-TPAT guidelines for ocean carriers recommend procedures for vessel security, manifest preparation, and similar issues; C-TPAT guidelines for importers focus on procedures that enhance the security of cargo (CBP, 2004).

The layered model also explains the basis of objections certain groups have to particular regulations. The World Shipping Council represents the ocean carriers' interests in Washington, D.C. In September 2003, the council issued a white paper that commented on various U.S. and foreign government programs to enhance supply-chain security (World Shipping Council, 2003). The council argued that carriers were not responsible for the contents of containers, an aspect of supply-chain security over which they cannot have full control. The shipper is responsible for loading and sealing a safe and secure container. Those who have custody of the container during its transit are responsible for its security in transit. Government also has critical responsibilities and, with the support of carriers and shippers, has expanded its capabilities to gather and analyze advance data on all container shipments, screen all such shipments, and inspect any container that raises a security question (World Shipping Council, 2003).

Several initiatives implementing RFID technology limit themselves to particular layers of the supply chain. The Smart and Secure Tradelanes Initiative has enlisted large shippers in the deployment of RFID tags and readers at the container level, tracking them with handheld and crane-mounted readers at ports and on vessels (2003). This initiative therefore focuses on improving the efficiency and security of the physical supply chain. Such retailers as Wal-Mart, Target, and the Albertsons grocery store chain are also embracing RFID technology but use it to track individual products and combat counterfeiting (Feder, 2004). RFID initiatives on the part of retailers fall squarely in the transaction layer of the supply chain.

⁶For complete program details, see CBP (2004).

SECTION 4

Capabilities of the Global Container Supply Chain

The stability of the global container shipping industry is based on efficiency and security: Any efforts to evaluate proposals for improving this system must compare them against both these properties. This requirement holds both for new applications of technology and for proposed modifications to shipping, customs, or trade policies. The ability of a supply chain to deliver goods efficiently and securely can be represented by five capabilities:

- **Efficiency.** The global container supply chain has evolved primarily to deliver goods more quickly and more cheaply than other modes of transport when volume and mass are taken into account.
- **Shipment Reliability.** The system must behave as expected, retrieving and delivering goods as directed with a minimum amount of loss due to theft and accident. Supply-chain shrinkage, resulting from misrouting and theft of goods, erodes both this trust and the efficiency of the shipping network. Misrouting causes losses through delays in shipment delivery. Theft results in both direct economic losses and indirect losses resulting from delays in product delivery.
- **Shipment Transparency.** The goods that flow through the global container supply chain must be legitimately represented to authorities and must be legal for transport. The system should be transparent enough to minimize improper use of the system. Traditionally, transparency has involved inspections at the port of entry to detect illegal immigrants or items being smuggled in an attempt to avoid regulations or tariffs. With homeland security currently receiving so much attention, the focus of exclusion has shifted to preventing terrorists from using the container shipping system to carry out attacks on the United States. Inspection at the port of entry can make it more difficult for terrorists to use containerized shipping as logistical support for moving people and supplies. However, inspections at the port of entry are less helpful for preventing terrorists from using containers as a means of attack (e.g., detonating a bomb aboard a ship arriving at port). Increased focus on the latter capability introduces new challenges.
- **Fault Tolerance.** Because the system is a network, problems at one node—such as a port—affect interconnected parts of the system. In unstable systems, a problem at a single node or link in the supply chain can bring the entire network to a halt. In fault-tolerant systems, the surrounding ports and distribution system can compensate when a section of the system is compromised. To the extent that neighboring ports and facilities are able to compensate for the loss of a port, the containerized shipping system is more fault tolerant.

- **Resilience.** Resilience is the ability of the supply chain to return to normal operations after a failure. For example, suppose that an oil spill occurs at a port. The response to contain the spill would impede the loading and unloading of ships, creating backlogs at the port and delaying shipments elsewhere. The more resilient the supply chain is, the quicker these backlogs will be cleared, avoiding the resulting delays. Resilience is a function of the system design and the response from the oversight layer.⁷

The first three of these capabilities are characteristics of the containerized shipping system when it is functioning normally. The final two, fault tolerance and resilience, are properties of the system's response to natural or intentional disturbances. The capabilities divide between efficiency and security. Efficiency is the only capability that directly reflects the cost, speed, and capacity of the system. All other capabilities are associated with supply-chain security.

Although these capabilities will be measured through distinctly different metrics, all five capabilities are interconnected. Gains in any one capability must be assessed with respect to comparative gains or losses in the others. For example, increasing inspections may improve security but increase delays at ports. Those making decisions about the design of and investments in security policies and technologies must assess the trade-offs among the five supply-chain capabilities and consider their relative importance in the context of specific decisions.

⁷ This is best illustrated by the Booz Allen Hamilton Port Security War Game, which estimated that closing the nation's ports for eight days would result in \$58 billion in economic losses (Gerencser, Weinberg, and Vincent, 2003).

SECTION 5

Managing Container Shipping Security: A Case of Technology-Induced Risk

A secure and efficient supply chain will be the product of an interconnected system of human and technological agents. How this complex system responds under normal conditions and following severe disturbances is a case of technology-induced risk. Technology-induced risk results from the operation of technology-dependent systems. Failures occur when system components fail to operate properly, interconnections are broken, or human error compromises operations. Such failures can either be random or the result of deliberate attack.

Interventions for managing technology-induced risk influence either exposures or effects (Morgan, 1981). Efforts to reduce event occurrence or the resulting exposures are akin to threat- or vulnerability-reduction strategies. In the context of supply-chain security, these strategies translate either to reducing the probability that an attack occurs or to reducing the probability that the attack is successful. Interventions that modify or reduce effects or compensate after the fact are consequence-reduction strategies.

In addition, it is important to consider human perceptions and values because this makes it possible to prioritize terrorism risks. It is also normatively preferable to direct preparedness resources toward the hazards about which society is most concerned. In addition, understanding society's perceptions and values presents opportunities (albeit limited) for reducing risks through public education and risk communication (Morgan, 1981). Given the potential trade-offs between security and efficiency, perceptions and values determine how much disruption of the container shipping system for the sake of improved security is acceptable.

Building Supply-Chain Capabilities

Stakeholders in the containerized shipping system have proposed multiple means of improving the system's security and efficiency. Several of these were introduced in Section 2. Some proposals are regulatory or policy fixes (such as C-TPAT and CSI) that impose administrative requirements through the customs inspection process. Others, such as MTSA, impose regulatory constraints on the system. Finally, shippers, carriers, customs organizations, and port operators are also looking for technological solutions for improving container security and efficiency, such as antitamper seals, RFID, x-ray and gamma-ray scanners, and remote sensors. The layered description of the global container shipping supply chain discussed in Section 3 and the supply-chain capabilities discussed in Section 4 provide a framework for assessing how these security measures are affecting the performance of the container shipping system. Working within this framework, the remainder of this section assesses the

programs covered in Section 2 from the perspective of technology-induced risk management. Table 2 summarizes this assessment.

As an example, consider deterrence, which plays an important role in the design of all policy and technology proposals for improving security. Each proposal is designed to make it more difficult to attack the containerized shipping system. The intended result is that targeting container shipping will be less attractive for thieves, smugglers, and terrorists. In this way, deterrence contributes to threat and vulnerability reduction. Deterrence, as discussed above, is not considered further in the following descriptions. However, it does play an important role in the design of each program.

Table 2 also offers a high-level view of how these objectives come together as an integrated strategy for port security strategy and whether there are any obvious gaps in the U.S. strategy. The table presents the capabilities that could be captured by private shippers, carriers, and port operators and the U.S. government; it does not highlight security benefits that might be realized at foreign ports. Also, this analysis does not answer the question of whether the aggregate response is sufficient. Further analysis, built on our framework, is required to address this question.

Customs-Trade Partnership Against Terrorism: Making Supply-Chain Participants Responsible for the Security of Container Cargo

C-TPAT is intended to improve efficiency through implementing processes and standards for participants in the transaction and logistics layers. Although C-TPAT is mandated by the Department of Homeland Security (i.e., the oversight layer), it is driven by requirements for the other layers.

As reflected in Table 2, C-TPAT does not make any clear contributions to supply-chain security aside from deterrence. In some cases, C-TPAT may make it more difficult for illicit cargo to be shipped via containers. However, this effect may be offset by the ability of terrorists and smugglers to game the system. This “carnival booth” effect has been described with respect to TSA’s computer-assisted passenger prescreening system (Martonosi and Barnett, 2004). C-TPAT also does not help reduce effects of events or mitigate them when theft, fraud, or terrorism occurs.

Operation Safe Commerce: Harnessing Technology to Improve Customs Inspection Effectiveness

OSC is an example of the oversight layer working with the logistics layer to improve supply-chain security at U.S. ports. Because OSC primarily addresses container screening and tampering technologies, it is not driven by the transaction layer.

This program might reduce fraud by improving detection at the port of entry. Similarly, Table 2 indicates that OSC might make it difficult for terrorists to use containerized shipping to supply comrades in the United States. However, OSC will not reduce the damage from a terrorist act, if an attack on the system is successful.

By the time containers reach ports, they are positioned for a terrorist attack. Thus, increased inspections will not reduce the exposure to or reduce the damages from attacks on

Table 2
Examples of How Preparedness Strategies May Influence the Exposure-Effects Chain of Notional Terrorist Events

Policy or Technology	Driving Layer	Anticipated Supply Chain Efficiency Effects	Anticipated Supply Chain Security Effects			
			Threat or Vulnerability Reduction	Reduce Probability of Attack	Reduce Probability of Successful Attack	Mitigate or Compensate for Consequences
Customs-trade partnership against terrorism	Transaction and logistics	Reduced shipping cost and time and increased volume; Expedited customs				
Operation Safe Commerce	Logistics and oversight		Reduced fraud: Detect at entry			
Container security initiative	Oversight			Reduced damage and fraud: Detect at origin		
Maritime Transportation Security Act of 2002	Oversight			Reduced theft: Control access		
Anti-tamper seals	Transaction and logistics				Reduced damage: Detect at origin	
Radio frequency identification	Transaction and logistics	Reduced shipping cost and time; Improved Logistics		Reduced damage, losses, and fraud: Deter terrorists, thieves, and smugglers	Reduced fraud: Detect at origin or entry	
X-ray and gamma-ray inspection	Logistics and oversight				Reduced theft losses: Detect unapproved transport	
					Reduced damage: Detect at origin	
					Reduced damage: Detect at entry or origin	
					Reduced damage: Detect at origin	
					Reduced damage: Detect at origin or entry	
					Reduced damage: Detect at origin	
					Reduced damage: Detect before cargo enters ports	

port facilities. Similarly, OSC does not reduce or modify the consequences of terrorist attacks or smuggling incidents if they are successful. Neither does it provide for compensation or mitigation to lessen the impact of losses from fraud, terrorism, or theft.

Container Security Initiative: Increasing Deterrence and Efficiency Through Cargo Inspection at Foreign Ports

CSI, an oversight-driven program, clears U.S.-bound containers at foreign ports. By increasing detection capabilities at the port of origin, CSI might improve the likelihood of detecting threats before they are onboard a ship bound for the United States. Thus, CSI could reduce U.S. exposure to losses from fraud and terrorism damage. This program might also reduce the processing time required at domestic ports of entry. However, because the program could increase processing time at the port of origin, it is not clear that a net improvement of efficiency will result.

Since CSI is solely focused on increased detection capabilities, Table 2 shows that it does not help decrease the effects of system hardening or mitigate the consequences of attacks.

Maritime Transportation Security Act: Reducing Theft and Improving Incident Response at Ports and on Vessels

MTSA is the response of the oversight layer to the threat of terrorist attack on the ports or U.S. vessels. Standardized port security and inspection protocols can reduce the costs of theft by controlling access to containers during transport. However, control at the port of entry will not reduce potential damages from terrorist attacks on ports from inbound containers. Making emergency response part of the port security plans can help increase the fault tolerance and resilience of the containerized shipping system.

None of MTSA's requirements clearly help improve the efficiency of the supply chain (see Table 2). In fact, the shipping industry has expressed some concern that its measures will increase shipping costs. In addition, MTSA does not institute measures that would affect the causes of damage or reduce the effects of theft, fraud, or terrorism.

Antitamper Seals: Improving the Integrity of Container Shipping

The transaction and logistics layers have driven the adoption of antitamper seal technology; the oversight layer has not mandated such technologies. As Table 2 indicates, antitamper seals might increase detection capabilities at ports of origin and ports of entry. Detecting tampering at the port of origin reduces the potential for damage to a U.S. port from either fraud or terrorism. Detection at ports of entry reduces only the potential damage from fraud. However, it is possible to breach a container without damaging many of the seals, thus circumventing the technology.

Antitamper seals are not intended to have significant effects on supply-chain efficiency. Any reductions in inspection or processing time would likely be modest and would

have to be balanced against the costs of the antitamper devices themselves. Antitamper seals will not modify the causes or help mitigate or compensate for effects when events do occur.

Radio Frequency Identification: Improving the Transparency of Supply-Chain Networks

As with antitamper seal technology, the transaction and logistics layers are driving adoption of RFID technology. However, unlike antitamper seals, RFID technology is expressly intended to increase efficiency.

RFID technology, as shown in Table 2, is intended to make the supply chain transparent, allowing carriers and shippers to track shipments from origin to destination. Through network transparency, shippers might see where bottlenecks occur in their supply chain and could potentially optimize shipping to improve supply-chain efficiency. Transparency can reduce the costs of theft and lost goods through early detection of misrouted or unapproved goods. Detection of inconsistencies in container contents, when observed at the port of origin, reduces both terrorism damage and fraud. Detection at the port of entry can decrease losses from fraud.

RFID also contributes to consequence reduction. Although RFID is not expected to modify the causes of effects, the ability to locate and reroute shipments rapidly following disasters improves supply-chain resilience.

X-Ray and Gamma-Ray Scanning: Improving Transparency of Cargo Shipments

Participants in the oversight layer have been the primary driver for scanning technologies, in an effort to keep dangerous goods out of the supply chain and to detect illegal cargo.

Using scanning technologies at foreign ports might reduce both losses from fraud and terrorism damage in the United States (see Table 2). Detection at the port of entry fundamentally reduces losses from fraud, although it may also reduce potential damage from terrorism significantly. For example, if a container is carrying a weapon intended for a specific target in the U.S. interior, detecting that weapon at the port of entry would allow it to be isolated and thus reduce the chance of significant damage.

Container scanning is not expected to improve supply-chain efficiency. In fact, scanning adds time to the processing of containers, and port operators or customs inspectors must bear the costs of the scanning equipment. Similarly, container scanning is not expected to help reduce consequence reduction because scanning does not mediate the effects of successful acts of terrorism.

Radiation Pagers, Portal Sensors, and Remote Monitoring: Increasing Capabilities to Detect Weapons of Mass Destruction

The oversight layer has also driven the adoption of remote-sensing technologies, such as radiation-warning pagers, portal radiation sensors, and remote-monitoring technologies. These systems detect radiation—new technologies may detect other agents—as the container

travels through the system. Detection at any point in the system hinders terrorists' ability to use container shipping as a weapon. However, as indicated in Table 2, detection must occur before containers reach the port of entry to prevent damage from attacks on the United States.

Improving detection capabilities at the port of origin provides the most significant reduction of potential terrorism damage to the United States. In addition, remote sensors that can detect weapons of mass destruction on ships before they reach port can also reduce terrorism damage.

Development of appropriate remote screening or portal sensors might also contribute to the detection of drugs or other misrepresented or illicit cargo. Currently, attention is mainly on the development of sensors for weapons of mass destruction. Sensors are not anticipated to improve supply-chain efficiency and do not mitigate or compensate for damages or losses when events do occur.

Preliminary Conclusions, Recommendations, and Future Inquiry

The global containerized supply chain is omnipresent. Thus, terrorist attacks on or using the supply chain could occur anywhere, and a well-planned attack could result in significant loss of life. In addition, the U.S. economy depends on the continued operation of the containerized supply chain: A successful attack on the supply chain could cause billions of dollars in damage to the U.S. economy (OECD, 2003; Pollack 2004). The threat of terrorist attacks using the container shipping system therefore demands policy attention.

The security of the supply chain can be considered a public good. Some who have not invested in these port security systems are likely to profit from the systemwide benefits (such as deterrence of terrorists and smugglers). It is not possible to prevent them from doing so, but their doing so does not diminish the benefits to those who did invest in the systems. On the other hand, this creates “free-rider” problems: Because those who do not invest will still benefit, the private sector may end up underinvesting in security. It may therefore be appropriate for government to step in to ensure the security of the global supply chain.

To this end, this report has developed a capabilities-based framework for assessing the security of the supply chain and determining areas where gaps in security remain. Our analysis has revealed some preliminary results and recommendations, as well as insights into several areas for further investigation.

Preliminary Conclusions

The analysis of supply-chain security and current efforts to improve it presented in the previous chapters leads to two conclusions. First, supply-chain efficiency and security are distinct but interconnected. Efforts to improve supply-chain efficiency may or may not affect the security of the system. Second, both public- and private-sector initiatives to improve the security of the global supply chain have focused largely on the prevention and deterrence of smuggling and terrorist attacks. Few initiatives have focused on improving the fault tolerance or resilience of the system.

The Inseparability of Supply-Chain Security and Efficiency

Improving the supply-chain’s efficiency may or may not improve its security. Increasing transparency to improve efficiency may also improve supply-chain security. Labor reductions for the sake of efficiency, however, may decrease security. Similarly, proponents of increased supply-chain security often cite increased efficiency as an auxiliary benefit, although the two properties are often independent. Other measures, such as increased inspections, could create delays that would lead to losses of perishable cargo or to negative economic effects on con-

signees. The interconnected nature of supply-chain capabilities suggest that security measures that reduce efficiency could have unintended negative consequences because stakeholders will look for ways to compensate for or circumvent the security requirements.

Specific examples abound. Product theft is a business risk for all users of the supply chain, and shippers and carriers have instituted policies to combat it. But the benefits of increased oversight and monitoring required to combat theft, or the processes recommended by CBP in the C-TPAT program, do not necessarily increase the efficiency of the supply chain.⁸ Actions that combat smuggling, likewise, have little effect on supply-chain efficiency; the smuggler's activities occur alongside normal business practices. Improving the two other properties of the supply chain, fault tolerance and resilience, does not increase efficiency and, under normal operating conditions, might work against it. Both these properties imply a certain amount of spare capacity, particularly at port terminals but also on ships and at transhipment points. Spare capacity, under normal operating conditions, is a misallocation of resources.

Potential Underinvestment in Fault Tolerance and Resilience

Most initiatives for securing the supply chain are public-sector efforts, focusing disproportionately on preventing terrorist attacks. In response to the attacks of September 11, 2001, CBP now views its primary role as fighting terrorism (Jacksta, 2004). Before then, CBP's principal regulatory roles were collecting duties and preventing smuggling.

Our analysis shows that few security enhancement programs seek to ensure either the fault tolerance or resilience of the system. As mentioned previously, these capabilities are a function of both the system design and the responses of participants in the oversight layer. In principle, it is in the best interests of a firm to plan for supply-chain failures. However, at the logistical level, additional capacity is incredibly capital intensive, and carrying it on a balance sheet makes little business sense.⁹

In 2002, the Port of Los Angeles and the Port of Long Beach handled 70 percent of all west-coast container traffic (Pacific Maritime Association, 2003). This concentration is a vulnerability created by the system's drive for efficiency. Were both ports to close for security reasons, the other west-coast ports, combined, lack the necessary infrastructure for absorbing all the traffic calling at Los Angeles and Long Beach. And they should not. However, incentives for development at smaller ports would create redundancy and excess capacity that would improve the fault tolerance and resilience of the container shipping system during an emergency. Because these incentives do not exist and receive little attention from members of the transaction or logistic layers, public investment will be needed to provide fault tolerance and resilience.

⁸ Since shipments and containers belonging to C-TPAT participants are granted expedited processing and clearance at U.S. ports of entry, CBP argues that the program increases supply-chain efficiency (Ginn and Lacy, 2004). This argument is misleading; participation in C-TPAT reduces the risk score that triggers an inspection but does not uniformly decrease the transit or dwell times of containers.

⁹ A Dutch Telematica Instituut study assumed that logistical operations are already optimized for efficiency because they are so capital intensive (Goedvolk et al., 2001).

Recommendations

These conclusions suggest three complementary paths for improving the security of the global container supply chain while maintaining its efficiency.

The Public Sector Should Seek to Bolster the Fault Tolerance and Resilience of the Logistical Supply Chain

The logistics level of the supply chain has distinctly private and public components: Ports are operated by private firms, such as P&O Nedlloyd and Hutchinson Port Holdings, and by port authorities; the freight rail network is largely privately owned and operated; and the interstate highway system is distinctly public. The closure of a major port—for whatever reason—would have a significant effect on the U.S. economy, and it is important to recognize that an appropriate response includes rerouting cargo to other available ports on some optimum basis and making plans for returning to normal operation. The government should lead the coordination and planning for such events for two reasons: First, the motivation of the private sector to allocate resources to such efforts is subject to the market failures of providing goods to the public; second, the government will be responsible for assessing security and decisions to close ports.

Security Efforts Should Address Vulnerabilities Along Supply-Chain Network Edges

Current efforts to improve the security of the supply chain focus on ports. MTSA and International Ship and Port Security codes specify a number of measures for controlling access to port facilities, monitoring the port area, and preparing for various emergency scenarios. Unfortunately, the route over which cargo travels is vast and difficult to secure, and many ports around the world had failed to follow the International Shipping and Port Security guidelines by the July 1, 2004, deadline. Tamper-evident seals and alarms can help identify compromised shipments, but, depending on the trade route, days or weeks may elapse before intrusions are detected. It is technologically possible to monitor the movement of all shipments in real time. Even though it is impossible to identify all illegal activity occurring in the supply chain, continued development of technologies to monitor network edges will help fill an important gap in the layered approach to container security.

R&D Should Target New Technologies for Low-Cost, High-Volume Remote Sensing and Scanning

Current sensor technologies for detecting weapons or illegal shipments are expensive and typically impose delays on the logistics system. As a result, security efforts have focused on technologies or processes for identifying containers that have been tampered with, for making it harder to tamper with containers, and for profiling containers to reduce the burden of volume on screening systems.

All these approaches have a common weakness: They are easy to circumvent. Tamper-resistant seals can be fooled. Profiling processes can be gamed as terrorists or smugglers learn what characteristics trigger profiling algorithms. New detection technologies for remote scanning of explosives and radiation would provide valuable capabilities for better securing the container shipping system. Technology planning must also be coordinated with market requirements for developing devices with low development and deployment costs.

Future Inquiry

This document is our initial assessment of the security of the global supply chain; we are continuing our work in several areas:

1. **Assessment of policies for improving supply chain security.** We have described a framework for assessing supply-chain security using a set of interrelated performance dimensions and a layered structure of the supply chain. The framework is readily applied to domestic and international policies and proposals, providing a consistent approach to evaluating their performance and security implications. Additionally, since the performance dimensions of fault tolerance and resilience are properties of the system as a whole, the framework allows quantitative assessment of appropriate public and private sector roles in protecting the supply chain.
2. **Systems analysis of supply-chain risk.** Modern business practices and the physical structure of the containerized supply chain conspire to amplify disruptions to the system. The framework described in this document can be applied to analyze sensitive nodes in the system and its critical paths, evaluate the systemwide effects of the adoption of new technologies, and determine procedures for “restarting” the system in the event that it must be shut down for security reasons.
3. **Technology assessment and research and development planning for improving supply-chain performance.** Research, development, and deployment programs continue for new technologies to improve supply-chain performance. The potential of these technologies to change the performance dimensions of the supply chain may now be evaluated; conversely, with knowledge of desired performance improvements, research and development planning may be undertaken to achieve them.
4. **Economic analysis of global trade trends in supply-chain performance.** The global supply chain is protean, and the roles of producing and consuming nations continue to shift. Extensions of this analysis include examining the competitiveness of particular trade lanes given regulatory changes to improve security and the study of the information flows among the transaction, logistics, and oversight layers required to support global trade and security.

References

Alling, Philip, Edward M. Wolfe, and Scott D. Brown, *Compliance Deadlines Loom: Supply-Chain Giants Drive Early Adoption of RFID*, New York: Bear-Stearns Equity Research, 2004.

Amaral, L. A. N., A. Scala, M. Barthelemy, and H. E. Stanley, "Classes of Small-World Networks," *Proceedings of the National Academy of Science*, Vol. 97, No. 21, 2000, pp. 11149–11152.

CBP—See U.S. Customs and Border Protection.

Cleeland, Nancy, Evelyn Iritany, and Tyler Marshall, "Scouring the Globe to Give Shoppers an \$8.63 Polo Shirt," *Los Angeles Times*, November 24, 2003, p. A1.

Cohen, Stephen S., *Economic Impact of a West Coast Dock Shutdown*, Berkeley, Calif.: University of California, 2002.

Feder, Barnaby J., "Wal-Mart Hits More Snags in its Push to Use Radio Tags to Track Goods," *The New York Times*, March 29, 2004, p. C4.

Flynn, Stephen E., "Beyond Border Control," *Foreign Affairs*, Vol. 79, No. 6, 2000, p. 57.

———, *America the Vulnerable*, New York: Harper Collins, 2004.

Ford, L. R., Jr., and D. R. Fulkerson, *Flows in Networks*, Princeton, N.J.: Princeton University Press, 1962.

General Accounting Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, Washington, D.C., GAO-03-770, 2003.

Gerencser, Mark, Jim Weinberg, and Don Vincent, *Port Security War Game: Implications for U.S. Supply Chains*, McLean, Va.: Booz Allen Hamilton, 2003.

Ginn, Michael, and Tamara Lacy, "An Overview of CSI and C-TPAT," paper presented at Maritime Homeland Security 2004, March, Miami Beach, Fla., March 29–31, 2004.

Goedvolk, Ernst-Jan, Bob Hulsebosch, Wil Janssen, and Piet Maclaine, *Risk Analysis of Container Import Processes: Security Risks Associated With Flows of Goods and Information in the Port of Rotterdam*, Version 1.2, Enschede, The Netherlands: Virtuele Haven, Telematica Institut, 2001.

Guare, John, *Six Degrees of Separation*, play, New York: Vintage, 1990.

Holmes, Bruce J., *Transportation Network Topologies, Network Theory: A Primer and Questions for Air Transportation System Applications*, Washington, D.C.: National Aeronautics and Space Administration, 2004.

IMO—See International Maritime Organization.

International Maritime Organization, Web site, 2004. Online at <http://www.imo.org/> (as of October 15, 2004).

Iritany, Evelyn, and Marla Dickerson, "Calculating Cost of West Coast Dock Strike is a Tough Act," *Los Angeles Times*, November 26, 2002.

Jacksta, Robert, "An Overview of U.S. CBP's Role in Maritime Homeland Security," paper presented at Maritime Homeland Security 2004, Miami Beach, Fla., 29–31 March, 2004.

Lloyd's List, When Security on Shore Compromises Safety at Sea, online broadsheet, April 28, 2004.

Machalaba, Daniel and Bruce Stanley, "In California, Santa's Goods Face Port Delays," *Wall Street Journal*, October 14, 2004, pp. B1–B2.

Martonosi, Susan E., and Arnold I. Barnett, "Security Profiling of Airline Passengers: How Effective Would It Be? Some Surprising Conclusions," working paper, Cambridge, Mass.: Massachusetts Institute of Technology, 2004.

Morgan, M. Granger, "Probing the Question of Technology-Induced Risk," *IEEE Spectrum*, Vol. 18, No. 11, 1981, pp. 58–64.

Nishiguchi, Toshihiro, and Alexandre Beaudet, "Fractal Design: Self-organizing Links in Supply Chain Management," in G. Von Krogh, I. Nonaka and T. Nishiguchi, eds., *Knowledge Creation: A Source of Value*, London: Macmillan, 2000.

Organisation for Economic Co-operation and Development, "Security in Maritime Transport: Risk Factors and Economic Impact," Maritime Transport Committee report, 2003. Online at <http://www.oecd.org/home/> (as of November 5, 2003).

Pacific Maritime Association, *Annual Report*, San Francisco, Calif.: Pacific Maritime Association, 2002.

_____, *Annual Report*, San Francisco, Calif.: Pacific Maritime Association, 2003.

Pelosi, Nancy, and Tom Daschle, "Pelosi and Daschle Deliver Pre-Bitull to State of the Union Address," Washington, D.C.: U.S. Senate, Office of the Democratic Leader, January 16, 2004. Online at <http://democrats.senate.gov/~dpc/releases/2004116B38.html> (as of October 26, 2004).

Pollack, Richard, *The Colombo Bay*, New York: Simon and Schuster, 2004.

Sheridan, Ralph, Interview regarding container security initiatives, Arlington, Virginia, 21 July, 2004.

Simchi-Levi, David, Philip Kaminsky, and Edith Simchi-Levi, *Designing and Managing the Supply Chain*, 2nd ed., New York: McGraw-Hill/Irwin, 2002.

Smart and Secure Tradelanes, "Phase One Review, Network Visibility: Leveraging Security and Efficiency in Today's Global Supply Chains," November 2003.

Stana, Richard M., "Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection," testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, Washington, D.C.: General Accounting Office, GAO-04-557T, 2004.

Technology Asset Protection Association, Web site, 2004. Online at <http://www.tapaemea.com> (as of October 15, 2004).

Transportation Security Administration, Operation Safe Commerce, Web page, 2004. Online at http://www.tsa.gov/public/interapp/asset_summary/asset_summary_0122.xml (as of October 15, 2004).

_____, "TSA to Test New ID Card for Transportation Workers," press release, August 10, 2004. Online at <http://www.tsa.gov/public/display?theme=44&content=09000519800c10bd> (as of October 15, 2004).

U.N. Conference on Trade and Development Secretariat, Container Security: Major Initiatives and Related International Developments, 2003. Online at <http://www.unctad.org/Templates/webflyer.asp?docid=4481&intItemID=1397&lang=1> (as of October 15, 2004).

U.S. Congress, 2002, Maritime Transportation Security Act, Public Law 107-295.

U.S. Customs and Border Protection, Enforcement: International Activities, Web site, undated. Online at http://www.cbp.gov/xp/cgov/enforcement/international_activities/csi (as of October 15, 2004).

_____, Import: Commercial Enforcement, Customs-Trade Partnership Against Terrorism, Web page, 2004. Online at http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ (as of October 15, 2004).

Wasem, Ellen, Jennifer Lake, Lisa Seghetti, James Monke, and Stephen Viña, *Border Security: Inspections Practices, Policies, and Issues*, Washington, D.C.: Congressional Research Service, 2004.

Watts, Duncan J., "Small Worlds: The Dynamics of Networks Between Order and Randomness," in P. W. Anderson, J. M. Epstein, D. K. Foley, S. A. Levin, and G. Meayer-Kress, eds., *Princeton Studies in Complexity*, Princeton, N.J.: Princeton University Press, 1999.

Wolfe, Edward M., Philip Alling, Harry D. Schwefel, and Scott D. Brown, *Track(ing) to the Future: The Impending RFID-Based Inventory Revolution*, New York: Bear-Stearns Equity Research, 2003.

World Shipping Council, *In-Transit Container Security Enhancement*, Washington, D.C.: World Shipping Council, 2003.

OCCASIONAL
PAPER

Protecting Commercial
Aviation Against the
Shoulder-Fired Missile
Threat

James Chow, James Chiesa, Paul Dreyer,
Mel Eisman, Theodore W. Karasik, Joel Kvirkly,
Sherrill Lingel, David Ochmanek, Chad Shirley

Approved for public release; distribution unlimited



INFRASTRUCTURE, SAFETY, AND ENVIRONMENT

The research described in this report was supported through provisions for independent research and development in RAND's contracts for the operation of Department of Defense (DoD) federally funded research and development centers: RAND Project AIR FORCE (sponsored by the U.S. Air Force), the RAND Arroyo Center (sponsored by the U.S. Army), and the RAND National Defense Research Institute (sponsored by the Office of the Secretary of Defense, the Joint Staff, the unified commands, and the defense agencies). The research itself was conducted within RAND Infrastructure, Safety, and Environment (ISE), a unit of the RAND Corporation. The mission of ISE is to improve the development, operation, use, and protection of society's essential built and natural assets; and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities.

Library of Congress Cataloging-in-Publication Data

Protecting commercial aviation against the shoulder-fired missile threat / James Chow ... [et al.].

p. cm.

"OP-106."

Includes bibliographical references.

ISBN 0-8330-3718-8 (pbk. : alk. paper)

1. Aeronautics, Commercial—Security measures. 2. Terrorism—Prevention. 3. Surface-to-air missiles.

1. Chow, James. 1966—

TL725.3.S44P76 2005

363.28'76—dc22

2004026555

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2005 RAND Corporation

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2005 by the RAND Corporation

1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138

1200 South Hayes Street, Arlington, VA 22202-5050

201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516

RAND URL: <http://www.rand.org/>

To order RAND documents or to obtain additional information, contact

Distribution Services: Telephone: (310) 451-7002;

Fax: (310) 451-6915; Email: order@rand.org

Preface

Following the terrorist attacks of 9/11, the question of whether or not to install countermeasure systems to protect commercial airliners against shoulder-fired missiles has been an issue of vigorous debate among decisionmakers in the United States and abroad. This research effort was designed to inform the American public and decisionmakers regarding the potential utility of technical countermeasures and other policies that could help to protect commercial aircraft against attacks with shoulder-fired missiles. We examine operational, effectiveness, and cost issues involved with countermeasure systems. During the course of our study, we had access to contractor and government information related to countermeasures and threat systems; however, all of our results and conclusions are based upon publicly releasable or open-source information.

In the period immediately following the September 11, 2001, attacks on the United States, the RAND Corporation undertook several research projects relating to counterterrorism and homeland security topics as elements of its continuing program of self-sponsored research. This research is the result of one of those research projects. The work was supported through the provisions for independent research and development in RAND's contracts for the operation of the Department of Defense (DoD) federally funded research and development centers: RAND Project AIR FORCE (sponsored by the U.S. Air Force), the RAND Arroyo Center (sponsored by the U.S. Army), and the RAND National Defense Research Institute (sponsored by the Office of the Secretary of Defense, the Joint Staff, the unified commands, and the defense agencies). The research itself was conducted within RAND Infrastructure, Safety, and Environment (ISE), a unit of the RAND Corporation. This mission of ISE is to improve the development, operation, use, and protection of society's essential built and natural assets; and to enhance the related social assets of safety and security of individuals in transit and in their workplaces and communities. Dr. Richard Neu, Assistant to RAND's President for Research on Counterterrorism (at the time this research was performed), provided overall supervision for this work.

Contents

Preface	iii
Figures and Tables	vii
Summary	ix
Acknowledgments	xiii
List of Abbreviations	xv
CHAPTER ONE	
Introduction	1
CHAPTER TWO	
The Threat: A Clear and Present Danger?	3
CHAPTER THREE	
Potential Economic Welfare Impact from an Attack	7
Estimating Shutdown Losses	7
Losses after Resumption of Airline Service	9
Summary and Caveats	9
CHAPTER FOUR	
Strategic Considerations	11
CHAPTER FIVE	
Policy Solutions and Operational Issues	13
CHAPTER SIX	
Countermeasure Systems	17
Flares	17
Laser Jammers	19
High-Energy Lasers	21
CHAPTER SEVEN	
Costs	23
Installation Costs	23

Operating and Support Costs.....	26
Budgetary Considerations	28
CHAPTER EIGHT	
Summary and Recommendations	31
Appendix A: Estimating Consumer Surplus Loss.....	35
Appendix B: Congressional Bills	41
References	45

Figures and Tables

Figures

2.1. Proliferation of MANPADS among Selected Non-State Groups	5
5.1. Protection Against MANPADS Provided at Many Levels	14
6.1. Summary of Potential Counters to MANPADS	22
7.1. FY 2004 Expenditures for DHS (billions of dollars)	29

Tables

3.1. Total Welfare Losses from a Systemwide Shutdown (in billions)	10
7.1. Total Airborne DIRCM System LCC Estimates (FY 2003 dollars, billions)	24
A.1. Aviation Miles by Trip Distance	36
A.2. Travel Costs for Air and Alternative Modes	37
A.3. Consumer Surplus Loss	39
A.4. Producer Surplus Loss	40

Summary

Air travel has become an integral part of modern life. Terrorists have long understood this and have made commercial aviation one of their prime targets. Al Qaeda and its affiliates have both the motive and the means to bring down U.S. commercial aircraft with shoulder-fired missiles, also known as man-portable air defense systems (MANPADS). No such attempt has yet been made against a U.S. carrier, but given the measures being taken to preclude 9/11-style attacks, the use of MANPADS will unavoidably become more attractive to terrorists.

What might be done to prevent such an attack? We concentrate here on the capabilities and costs of onboard technologies to divert or destroy an attacking missile. Given the significant costs involved with operating countermeasures based upon current technology, we believe a decision to install such systems aboard commercial airliners should be postponed until the technologies can be developed and shown to be more compatible in a commercial environment. This development effort should proceed as rapidly as possible. Concurrently, a development effort should begin immediately that focuses on understanding damage mechanisms and the likelihood of catastrophic damage to airliners from MANPADS and other forms of man-portable weapons. Findings from the two development programs should inform a decision on the number of aircraft that should be equipped with countermeasures (from none to all 6,800 U.S. jet-powered airliners) and the sequence in which aircraft are to be protected.

If it is determined that U.S. commercial airliners should be equipped with countermeasures upon completion of the development program, they should be employed as part of a broader set of initiatives aimed at striking and capturing terrorists abroad, impeding their acquisition of missiles, and preventing them and their weapons from entering the United States. Attention should also be paid to keeping MANPADS-equipped terrorists out of areas adjacent to airports and improving commercial airliners' ability to survive fire-induced MANPADS damage.

A multilayered approach is important because no single countermeasure technology can defeat all possible MANPADS attacks with high confidence. Nonetheless, substantial protection can be achieved. Laser jammers, for instance, will be commercially available for installation aboard airliners soon and should be able to divert single or possibly dual attacks by the relatively unsophisticated MANPADS accounting for most of those now in the hands of terrorists. Ground-based high-energy lasers (HELs) intended to destroy approaching missiles could counter MANPADS of any degree of sophistication, but they are not ready for deployment in the next few years and have significant operational challenges to overcome. Pyrophoric flares used reactively offer the promise of a cheaper alternative with better potential to handle

multiple attacks than laser-based systems, but their effectiveness at protecting large transport aircraft from any MANPADS attack is not well established, and they would be most likely ineffective against sophisticated future systems.

We estimate that it would cost about \$11 billion to install a single laser jammer on each of the 6,800 commercial aircraft in the U.S. fleet. The operating costs of fleetwide countermeasures will depend on the reliability of the system. Extrapolating from early reliability data from the systems currently deployed on large military aircraft, the operating and support (O&S) costs for a commercial variant were assessed to be \$2.1 billion per year for the entire commercial fleet. The full ten-year life-cycle costs (LCCs) for developing, installing, operating, and supporting laser-jammer countermeasures are estimated to be \$40 billion. If reliability goals recommended by the Department of Homeland Security (DHS) can be achieved, the ten-year LCCs are estimated to be \$25 billion.

When would such an investment be worth it? That is not a question answerable solely through quantitative analysis, but some light can be shed by four avenues of inquiry. First, what would be the likely economic costs of a successful attack? If we take into account the value of a lost aircraft and a conventional economic valuation of loss of life, the *direct* cost would approach \$1 billion for every aircraft downed. The indirect economic damage from an attack would be far greater. These costs result from the loss of consumer welfare through preemption of a favored travel mode or reluctance to use it, as well as operating losses suffered by airlines subsequent to an attack. These amounts will depend primarily upon two factors: the length of any possible systemwide shutdowns in air travel and any kind of longer-lasting public reluctance to fly. Both factors are difficult to predict, but if air travel were shut down for a week (it was shut down for three days after 9/11), the economic loss would amount to roughly \$3 billion during the shutdown itself. Extrapolating from the long-term effects of the 9/11 shutdown, losses over the following months might tally an additional \$12 billion, for a total economic impact of more than \$15 billion.

A second avenue of inquiry can help place the cost of MANPADS countermeasures in context. To what extent must homeland-security and other counterterrorism resources be expanded or diverted to fund this one effort to help respond to a single threat? The \$2.1 billion annual O&S cost, should it be borne by the government, amounts to only about 6 percent of the annual DHS budget. The fraction is much smaller if the costs of operations in Iraq and Afghanistan are included in the base. However, the \$2.1 billion is a substantial fraction of total current federal expenditures on transportation security.

Third, it must be recognized that loss of life and economic impact would not be the only costs of a MANPADS attack. The perceived inability of the U.S. government to prevent attacks on its citizens on its own soil would set back U.S. efforts to counter terrorist groups globally and could weaken U.S. influence across a range of other interests abroad. Such an attack would also cause unquantifiable losses of security among the U.S. populace.

Fourth, and lastly, while countermeasures have been demonstrated to be an effective resource in protecting our military aircraft, the circumstances of protecting commercial airliners from terrorists are sufficiently different that we should ask ourselves the following questions: Upon deployment of countermeasures, how easy do we think it will be for terrorists to adapt and find vulnerabilities to airliners through the use of weapons that are not affected by counter-

measures? Would defenses against these weapons be possible, or would they require a similar level of funding to protect against?

A decision as to whether to proceed with a MANPADS countermeasure program must thus balance a variety of considerations. On the plus side:

- New countermeasure technology with capability against a variety of attack situations will be available in the near term, with the potential to avert the loss of hundreds or even thousands of lives and tens of billions of dollars.
- Funding such a system would require a reallocation or expansion of federal homeland-security resources of perhaps 5 percent—and a much smaller proportion of total federal counterterrorism resources.

On the minus side:

- Annual operating costs would represent nearly 50 percent of what the federal government currently spends for all transportation security in the United States.
- Well-financed terrorists will likely always be able to devise a MANPADS attack scenario that will defeat whatever countermeasures have been installed, although countermeasures can make such attacks considerably more difficult and less frequent.
- Installing countermeasures to MANPADS attacks may simply divert terrorist efforts to less protected opportunities for attack. To put it another way, how many avenues for terrorist attack are there, and can the United States afford to block them all?

Given the significant uncertainties in the cost of countermeasures and their effectiveness in reducing our overall vulnerability to catastrophic airliner damage, a decision to install should be postponed, and concurrent development efforts focused on reducing these uncertainties should proceed as rapidly as possible. The current DHS research, development, test, and evaluation (RDT&E) activities are a prudent step both toward reducing significant cost uncertainties involved and minimizing the delay of program implementation once a go-ahead decision is reached.

To summarize, any federal policy to protect against MANPADS should not be restricted to countermeasures development, but should involve multiple layers, with emphasis on the following areas:

1. Rapidly understanding and finding ways to reduce the O&S cost component of countermeasures in a commercial-airline setting. In addition, decisionmakers should be thinking about how specific countermeasure systems would work best in conjunction with other protection efforts and technologies. Understanding the weaknesses of countermeasures should help focus these efforts, and vice versa.
2. Focusing a concurrent technology development effort on understanding damage mechanisms and the likelihood of catastrophic damage to airliners from MANPADS and other forms of man-portable weapons such as rocket-propelled grenades (RPGs), mortars, and small-arms fire. This will serve three purposes: clarifying the damage caused by single or

multiple MANPADS hits on airliners, informing choices regarding the implementation of mitigating measures such as inerting fuel tanks and missile countermeasure systems, and assessing the seriousness of other forms of attack against airliners.

3. Working with international governments to slow down the proliferation of MANPADS technologies, in particular those against which countermeasures are less effective.
4. Putting together concepts of operation that integrate countermeasures into the overall aviation safety, security, and law enforcement system. These can help local law enforcement establish the size and location of airport security perimeters and define ways in which information from the onboard countermeasure system sensors can be used to help find, track, and apprehend MANPADS operators. Lastly, they would help provide an understanding of the costs from false alarms to air-traffic operations and local law enforcement.

Acknowledgments

The authors would like to extend thanks to Richard Neu, Natalie Crawford, and Jim Thomson of RAND for their support and feedback during this effort. Other RAND staff providing valuable feedback included Bruce Hoffman, Russ Shaver, Brent Bradley, Tim Bonds, Tom Hamilton, Claude Berrebi, Charlie Kelley, and Richard Mesic. Discussions with numerous external parties provided a diverse set of inputs and greatly improved our understanding of the relevant issues. These parties included Patrick Bar-Avi (Rafael USA), Mike Barrett (NAVAIR), Christopher Bolckom (Congressional Research Service), Richard J. Doubrava (ATA), Anthony R. Grieco, Elizabeth Gurin (GAO), Yael Hiram (Rafael USA), Ernest "Burt" Keirstead III (BAE), Robert Kudwa (Kudwa and Associates), Igo Licht (IAI), Dave McNeely (Boeing), Alvin D. Schnurr (Northrop Grumman), David Snodgrass (Northrop Grumman), John Stanfill (Northrop Grumman), Jim Tuttle (DHS), and Col. Tal Yeshaya (Embassy of Israel). Finally, all omissions or mistakes are the sole responsibility of the authors.

List of Abbreviations

AUPC	average unit production cost
C ²	command and control
CG	command-guided
CLIRCM	closed-loop infrared countermeasure
CRAF	Civil Reserve Air Fleet
DHS	U.S. Department of Homeland Security
DIRCM	directed infrared countermeasure
DoD	U.S. Department of Defense
FAA	Federal Aviation Administration
FOC	full operational capability
FOV	field of view
FPA	focal plane array
FRP	full-rate production
FY	fiscal year
GDP	gross domestic product
HEL	high-energy laser
IR	infrared
IRCM	infrared countermeasure
IRST	infrared search and track
LAIRCM	large-aircraft infrared countermeasure
LAX	Los Angeles International Airport
LCC	life-cycle cost
LRIP	low-rate initial production
MANPADS	man-portable air defense systems
MEMS	micro electro-mechanical system
MTBF	mean time between failure
MTHEL	mobile tactical high-energy laser
MWIR	mid-wave infrared
MWS	missile-warning system
O&S	operating and support
PB	President's Budget

RDT&E	research, development, test, and evaluation
RF	radio frequency
RPG	rocket-propelled grenade
SAM	surface-to-air missile
SOF	Special Operations Force
UAV	unmanned aerial vehicle
UV	ultraviolet

CHAPTER ONE

Introduction

Travel and tourism is now the world's largest industry. American commercial air carriers alone generate over \$100 billion in revenue annually and account for 720,000 jobs. Directly related industries, including commercial-aircraft production and airport services, generate an additional \$50 billion and 375,000 jobs.¹ More broadly, air travel has become, for many Americans, an integral part of their professional and personal lives. In 2000, passengers on U.S.-owned commercial air carriers took more than 600 million trips.² Clearly, a credible threat to the viability of America's commercial airline industry could have profound effects on the nation's economy and on Americans' way of life.

Shoulder-fired missiles (also sometimes called man-portable air defense systems [MANPADS]), such as the U.S.-made Stinger, pose such a threat. These systems are relatively inexpensive, widely available in the international weapons marketplace, and lethal to aircraft lacking countermeasures. They offer terrorists a means of bringing down airliners at any airport and thus have the potential to induce air travelers to think that they are not safe anywhere.

This paper is intended to assist policymakers in formulating appropriate responses to the threat posed by MANPADS in the hands of terrorist groups. Specifically, we address the question of whether the U.S. government should develop and deploy countermeasure systems to protect commercial aircraft from such missiles and, if so, what types of systems merit consideration.³

The paper addresses the following topics:

- the nature and severity of the threat posed by terrorist groups with MANPADS and the potential economic consequences of missile attacks on U.S. commercial aircraft
- the MANPADS threat in the context of the broader war on terrorism
- operational and tactical aspects of the threat, including potential operating areas around major airports and options for limiting terrorists' access to weapons and potential targets

¹ Wilbur Smith Associates, "The Economic Impact of Civil Aviation on the U.S. Economy," www.wilbursmith.com/Economic_Impact_of_Civil_Aviation_on_the_US_Economy.pdf, accessed 5/1/03.

² That is, there were 600 million "revenue emplanements" on American air carriers in 2000. Air Transport Association, Office of Economics, Airline Industry Facts, Figures, and Analyses, <http://www.airlines.org/econ/d.aspx?nid=1026> (as of March 1, 2003).

³ At the time of writing, the Department of Homeland Security (DHS) is leading the Counter-MANPADS Air Defense System Development and Demonstration effort, aimed at migrating available military technologies that could best protect commercial airliners from MANPADS. The two-year effort began in October 2003 and is intended to result in recommendations to the administration and Congress on how to proceed. In addition, there were two congressional bills recently introduced related to the installation of countermeasures aboard commercial airliners (see Appendix B).

- the characteristics and limitations of technical options available for countering missiles once they have been launched
- the potential cost of developing, installing, and maintaining candidate countermeasure systems, along with a consideration of who should bear the costs
- recommendations regarding how to proceed

The Threat: A Clear and Present Danger?

Just how serious is the threat posed by MANPADS in the hands of terrorists? Terrorist threats, by their very nature, are difficult to evaluate precisely. Enemy groups are constantly mutating, seeking to master novel capabilities, recruiting new foot soldiers, shifting locations, changing leaders, plotting different attacks. Under pressure from United States and allied security agencies, al Qaeda and related organizations may lose capacity in one dimension but gain in another. Factors such as these make it difficult to predict terrorist attacks with any specificity. However, it seems prudent for decisionmakers responsible for homeland security to regard the probability of an event as high when those who would perpetrate it have, at once, the motive, means, and opportunity to carry out the act. Do they?

Motive. This, at least, seems clear: terrorists from al Qaeda and its affiliates want to kill Americans, and they want to do so in spectacular ways.¹ Since the 1970s, international terrorists have exhibited a particular fascination with commercial aircraft, which are regarded as symbols of Western technological prowess. Bin Laden and his lieutenants must also recognize the strategic value of attacking Americans in their homeland. The U.S. response to al Qaeda's killings of Americans in Saudi Arabia, Africa, and Yemen prior to 9/11 was rather restrained. The reactions to 9/11 were anything but. Attacks on the American homeland have the potential not only to create larger numbers of U.S. casualties but also to yield much greater economic effects in this country than attacks overseas. Furthermore, occurring as they do under the very noses of U.S. security agencies, they can have profound effects on Americans' sense of security and well-being. In light of this, we judge that al Qaeda's leaders would relish the opportunity to bring down American commercial aircraft full of passengers, preferably in daylight and in cities that are major media hubs. Although they would expect to get the most value out of attacks perpetrated in the United States, they would also regard as useful the ability to attack American airliners abroad.

¹ While that is clear and sufficient for our purposes, it begs the larger question of *why* terrorists seek to kill Americans. Their own statements on this issue are not very enlightening. The leaders of al Qaeda and similar groups claim that they conduct such attacks in the name of Muslims everywhere in pursuit of objectives that have shifted somewhat over time. Prominent among these have been to force the United States to withdraw its military forces from the Middle East and to abandon its support of pro-Western governments there, to expel Israel from occupied territories, to overthrow secular governments in Muslim lands, and to reestablish the Caliphate. To those not in thrall to radical Muslim ideology, no meaningful connection between these millennial goals and specific terrorist attacks is discernible. Rather, at a practical level, the killing is undertaken both for its own sake (these people are professional murderers) and for reasons of institutional vitality. Terrorist organizations, like legitimate enterprises such as businesses, foundations, and universities, compete for money, talent, and influence. In the terrorist world, these goods tend to flow to groups that demonstrate frequently their potency as instruments for striking out against the enemy. See D. Benjamin and S. Simon, *The Age of Sacred Terror*, New York: Random House, 2002, pp. 156–66.

Means. Al Qaeda and many other groups hostile to the United States have MANPADS and the ability to use them. Over 700,000 MANPADS have been produced worldwide since the 1970s.² The United States and other countries provided MANPADS to mujahideen fighters in Afghanistan during the 1980s, along with hands-on training to ensure that they could be used effectively (which they were). Many thousands of MANPADS, including some Stingers sent to Afghanistan, are said to be unaccounted for worldwide. During the recent U.S. operations in Afghanistan, Russian SA-7s and British Blowpipes were recovered from Taliban caves in Afghanistan. SA-7s and other Russian-made models can be purchased in arms bazaars in a number of Middle Eastern and Central Asian countries. In some of these markets, such systems are sold for as little as \$5,000.³ With the increase in collaboration among terrorist groups, one may expect the transfer of a variety of MANPADS types among them. Figure 2.1 provides an overview of non-state groups known or thought to be in possession of MANPADS today.⁴ Al Qaeda in particular has at least first-generation MANPADS, has the ability to move them about internationally, and has decided to employ MANPADS attacks as part of its terror campaign. That was shown, for example, by the November 2002 attempt to use two MANPADS missiles to bring down an Israeli charter airliner departing Mombasa, Kenya.

Opportunity. Herein lies the question. Creating opportunities for attacks means smuggling one or more missile systems and trained operators into either the United States or, failing that, a country regularly served by an American carrier, and positioning them for a high probability-of-kill shot against an arriving or departing flight. The fact that no known attempts have yet been made against a U.S. civil carrier suggests either that the required assets are not in place or that al Qaeda's leaders are waiting for what they regard as a more propitious time to undertake such attacks.

The difficulties associated with getting the assets in place are certainly not insurmountable for an organization such as al Qaeda. The difficulties and risks associated with smuggling a handful of man-portable weapons and a few trained operators into the United States (or neighboring countries regularly served by U.S. carriers) are probably commensurate with those of training, indoctrinating, and positioning the four teams of men who commandeered and flew the aircraft involved in the attacks of September 11. As their name suggests, these weapons are small and lightweight (less than 40 pounds). They could easily be smuggled into the United States in a packing crate inside one of the 20,000 uninspected shipping containers that are unloaded at U.S. ports every day or by a variety of other means.⁵

MANPADS have already been used by terrorists and other operatives against a variety of aircraft in many parts of the world, including Africa, Asia, and Central America. One source

² CSIS, "Transnational Threats Update," Vol. 1, No. 10, 2003.

³ Jane's Terrorism and Insurgency Centre, "Proliferation of MANPADS and the Threat to Civil Aviation," August 13, 2003, http://www.janes.com/security/international_security/news/jtic/jtic030813_1_n.shtml (as of November 1, 2003).

⁴ See D. Kuhn, "Mombassa Attack Highlights Increasing MANPADS Threat," *Jane's Intelligence Review*, Vol. 15, No. 2, 2003, pp. 26-31. See also T. Gusinov, "Portable Missiles May Become Next Weapon of Choice for Terrorists," *Washington Diplomat*, June 16, 2004; and P. Caffera, "U.S. Jets Easy Target for Shoulder-Fired Missiles," *San Francisco Chronicle*, November 30, 2002, p. A14.

⁵ An interesting example of an alleged MANPADS smuggling ring involves the ongoing case of the British national Hemant Lakhani. According to prosecutors, Lakhani agreed to deliver an SA-18 missile to U.S. agents posing as buyers after he obtained it from Russian agents posing as sellers. CNN, "Feds Tell How the Weapons Sting Was Played," CNN.com, August 14, 2003, <http://cnn.com/2003/LAW/08/13/arms.sting.details/> (as of November 3, 2004).

Figure 2.1
Proliferation of MANPADS among Selected Non-State Groups

Different MANPADS classes available on black and grey markets

- 1st gen infrared – Reticle Scan, SA-7
- 2nd gen infrared – Conical scan SA-14, SA-16, Basic Stinger
- 3rd gen infrared – Pseudo imaging, SA-18
- CG – Command guided, Blowpipe



RAND OP106-1

estimates that of the 35 recorded attacks against civilian aircraft, 24 planes were shot down, killing over 500 people.⁶ Most of these attacks, however, were against non-jet-powered aircraft, such as helicopters and turboprop and piston-engine aircraft. This same source lists only five incidents where large jet-powered airliners were believed to have been attacked by MANPADS, including the attack on the Israeli jet in Kenya. Of these, two of the five resulted in catastrophic losses. Most recently, in November 2003, a DHL Airlines Airbus 300 was damaged by a MANPADS while flying near Baghdad International Airport, but managed to return safely without loss. No attempts have been recorded against a U.S. commercial airliner.

Given the motive to attack commercial airliners with MANPADS, the means to do so, and the opportunity to bring weapons and operators into the United States, why have we not already witnessed attempted attacks on American commercial airliners? One answer seems to be that the terrorist leadership has thus far regarded other means of killing Americans as more attractive. Because commandeering an airliner and crashing it into a large building was feasible, this tactic was preferred because it would not only undermine Americans' confidence in flying but also would produce far more destruction on the ground. However, as measures are taken to preclude 9/11-style attacks (e.g., improvement in screening at airports, deployment of air marshals on aircraft, strengthening of cockpit doors), attacking aircraft with MANPADS will unavoidably become more attractive to terrorists.

⁶ There are various estimates of these totals. The quoted numbers are taken from C. Bolckom, B. Elias, and A. Feickert, *Congressional Research Service Report for Congress: Homeland Security: Protecting Airliners from Terrorist Missiles*, 2003.

Potential Economic Welfare Impact from an Attack

Threats to commercial aviation are numerous and varied, and the cost of instituting preventive measures for all of these threats could become quite large. A sense of the economic impact of an attack affords some context for the allocation of resources to countermeasures. Economic losses may be divided into three categories: immediate, tangible losses from the attack; losses to travelers and airlines during a subsequent air-travel shutdown (as after the 9/11 attacks); and losses to travelers and airlines from reduced demand once the industry resumes operations.

Initial damages from such an attack would likely approach \$1 billion per aircraft destroyed. These are straightforwardly estimated. Larger aircraft typically cost \$200–250 million (depending on the exact model) and carry around 300 passengers each. Monetizing the value of the lives of the passengers aboard is always an uncomfortable calculation, and no earthly compensation can restore the loss of a loved one. But to make the tradeoffs that must be made in other situations between lives and resources, compensation policies and other economic treatments typically approximate a value per life of \$2–2.5 million.¹

In the aftermath of September 11, commercial air travel was stopped entirely for a few days and was severely disrupted for at least a week before flight schedules returned to something even close to normal. We infer that shutdowns of individual airports and the whole system are a possibility if a MANPADS attack were to be successful. In the remainder of this section, we show how we estimated shutdown losses—first for travelers and then for the airlines—and losses after resumption of operations.

Estimating Shutdown Losses

Beyond the immediate destruction of life and property, the economic impact of a MANPADS attack can be characterized in different ways. One ramification is the potential change in gross domestic product (GDP) that may result from the airline shutdown itself, from slowdowns in industries associated with the airlines, and subsequently from changes in people's behavior. Lower demand for air travel may lead to less spending on other kinds of goods and services

¹ The September 11 Victim Compensation Fund made an average death claim payment of about \$2.1 million. See Department of Justice, September 11th Victim Compensation Fund of 2001: Compensation for Deceased Victims, http://www.usdoj.gov/victimcompensation/payments_deceased.html (as of January 5, 2004). See also L. Dixon, *Assistance and Compensation for Individuals and Businesses after the September 11th Terrorist Attacks*, Santa Monica, Calif.: RAND Corporation, MG-264-ICJ, forthcoming.

in the economy, such as fewer stays at hotels and decreased business travel. Aircraft manufacturers (at home and abroad) may be adversely affected, too. However, while some activities may decline, others may increase. Domestic travel destinations may replace international ones. Individual cities or regions may be affected in different ways, but losses in some areas will be offset to some extent by gains in others.

We have chosen an alternative way to value the economic impact—through a measure of economic welfare. Economic welfare captures aspects of the value of air travel that may not be captured in GDP. Economic welfare is made up of consumer and producer surplus. The value consumers attach to the goods and services they buy is *at least* what they paid for them, or they would not have bought them. Consumer surplus is the excess of that value over the price. Analogously, producer surplus is the difference in value between what is paid to companies for a service (or good) and what it costs companies to produce that service. In this context, the welfare change is the change in the surplus value of transportation to air travelers and the change in profitability of the airline industry.

Consumer surplus may be understood intuitively as follows. Someone may pay \$350 to fly round-trip across the country, but that person might have been willing to pay up to \$500 for that service. The difference between what was paid for the service and how it was valued is the surplus the consumer gains from the trip—in our simple case, \$150. The importance of consumer surplus is that if an attack happened and air travel were shut down, or if the airlines continue to fly but the traveler does not feel comfortable flying, the consumer in our example would be willing to pay \$150 to be able to fly again with the system the way it was before. In that sense, the consumer values the loss of air travel (or his or her concern over its safety) at \$150 for that trip.

To estimate the actual consumer surplus for a successful shoot-down of a commercial aircraft in the United States, we first divide air travel into different market segments based on length of trip. Then we estimate the cost of travel for different travel modes, including air travel and its alternatives, in these market segments. We examine travelers' willingness to pay to avoid the shutdown of air travel, which varies by segment, and calculate the consumer surplus loss that results. (For details of the consumer surplus estimate, see Appendix A.) We estimate that, in the event of a one-week airline shutdown, a consumer surplus loss of \$2.0 billion would accrue; during a month-long shutdown, the loss would amount to \$8.4 billion.

Producer surplus is defined as the difference between revenue and costs. Because passenger revenue should approximate passenger costs during normal operations in a competitive industry, we ignore lost profits in our calculations.² However, a systemwide shutdown would mean a number of costs with no revenue to offset them.

For short-term disruptions of a day or a week, we assume that contracts will obligate labor and capital costs (including leases on aircraft) to be paid. Only fuel costs would be saved,

² In economics, a competitive industry theoretically yields zero “excess” profit—that is, profit above and beyond a normal rate of return experienced across industries. This result holds because if these excess profits exist, new entrants will join a market and compete those excess profits away, until there is no greater incentive to join the industry in question than any other industry. A normal rate of return remains, but this just offsets the cost of capital (and usually compensates for the risk of the investment). Figures from the 2002 Annual Report of the Air Transport Association show that its member airlines earned a net profit of 1.3 percent of revenue over the period 1991–2000.

as planes would not be flown, but all other costs during this period would be lost. With a shutdown of a month, food expenditures might be avoided, but once again capital and labor and all other non-fuel costs would be counted as losses. With those assumptions, we estimate producer losses of \$1.4 billion for a one-week shutdown and \$5.6 billion for one month. The combined welfare loss (consumer and producer surpluses) would thus come to \$3.4 billion for a one-week shutdown and \$14.0 billion for one month.

Losses after Resumption of Airline Service

Once airline operations resume following a shutdown, a significant amount of air travel may still be deterred through fear of flying, changes in airline operating schedules, and the increased inconvenience of additional security measures. That represents a loss to society in the form of further decreases in consumer and producer surplus. Reductions in future travel should be greater the longer the systemwide shutdown is. We assume that a shutdown of a day would reduce the number of flyers by 10 percent of normal in the following two-week period, with the corresponding loss.³ A shutdown of a week would affect 15 percent of the travel for the next six months. And a one-month shutdown is taken to reduce travel for the next year and a half by 25 percent.

This 10–15 percent net reduction in travel corresponds roughly with the experience of the airline industry in the aftermath of the prohibition of travel for more than a day but less than a week after September 11. Airline layoffs announced through February 2002, six months after the system shutdown, were 14 percent of employment. And a year later, air travel was still down about 8 percent, although some of this decline is certainly due to a general slowdown in the economy.

These future losses from reduced demand for air travel can be quite large, larger in fact than the loss during the period of shutdown because the fear and uncertainty driving them lasts much longer than the shutdown. We estimate that the country would be willing to pay \$12 billion to avoid an incident that would seriously affect travelers' confidence for the next six months. That value increases to over \$50 billion for an incident that would affect travel for a year and a half. Admittedly, these future loss factors are somewhat speculative.

Summary and Caveats

In summary, then, based on the effects of the attacks of September 11, we find it plausible that demand for air travel could fall by 15–25 percent for months after a successful MANPADS attack on a commercial airliner in the United States. A weeklong systemwide shutdown of air travel could generate welfare losses of \$3–4 billion, and when losses from reduced air traffic in the following months are added in, the result could exceed \$15 billion (see Table 3.1). By *losses*,

³ This 10 percent is a net reduction in air travelers. Some travelers who were scheduled to fly during the shutdown will resume their intended travel after the shutdown ends, but the net reduction is 10 percent. Also the distance pattern of flights taken is assumed to remain stable—that is, no shift to shorter or longer routes.

Table 3.1
Total Welfare Losses from a Systemwide Shutdown (in billions)

	One Day	One Week	One Month
Consumer Surplus Loss	\$0.3	\$2.0	\$8.4
Producer Surplus Loss	\$0.2	\$1.4	\$5.7
Direct Loss Subtotal	\$0.5	\$3.4	\$14.1
Future Loss Factor	10%	15%	25%
Indirect Loss Subtotal	\$0.9	\$12.4	\$56.6
Total Loss	\$1.4	\$15.8	\$70.7

we mean that airlines and the traveling public would be willing to pay that much to avoid a catastrophic attack on air transportation. Note that the amount is not MANPADS-specific; it represents the willingness to pay to avoid such an attack from any source of terrorist threat, be it MANPADS attack, hijacking, bombing, or other. If the public reluctance to fly were less severe or lasted for a shorter period of time following an attack (say, because of specific countermeasures to the threat that could be rapidly adopted), the welfare loss would be less. If the public reaction were even greater, the welfare loss could be even more.

A few other caveats to this economic analysis are in order. The analysis does not attempt to address any issues of local traffic congestion from changes in travel patterns. Nor does it account for the possibility that passengers may be willing to pay more per hour to avoid additional travel time as trips get longer; without specific data to rely upon, we presume these per-hour values to be uniform across all trip distances. Our estimates of consumer surplus loss depend on elasticity calculations—that is, estimates of the responsiveness of demand to price changes. These are best applied in a narrow range around the values for which they are estimated. The system shutdown scenarios produce effective price increases well outside of the typical range faced by business and leisure travelers. The use of the elasticity estimates here is done in the absence of either better data (or a more robust theory of traveler reaction to safety concerns) to inform the calculation, and this use is best confined to estimating an order of magnitude of results rather than attributing accuracy to specific numbers.

Finally, losses during a shutdown and following resumption of service are likely to be strongly conditioned by the success of law enforcement at apprehending MANPADS operators and their supporters. If arrests are made, federal officials can credibly assure the public that air travel is safe, and no further attacks follow the resumption of service, economic losses may be no greater than those shown here for a shutdown that might be as short as a week. If one or more of those conditions is not met, a longer or repeated shutdown and disproportionately larger post-resumption losses may accrue.

Strategic Considerations

Decisions regarding the installation of countermeasures aboard airliners must be considered within the context of the larger war on terrorism being waged by the United States and like-minded governments around the world. Al Qaeda and groups with similar capabilities and agendas constitute a serious threat not only to the safety and well-being of Americans but also to America's position in the world. Global-reach terrorism and the battle against it is seen as a contest played out on several fields at once in which the audience is global and the primary stakes are psychological. Both sides try to shape the perceptions of this global audience: terrorists seek to convince people that their cause is just and worthy of support; responsible governments seek to spread the conviction that terrorist attacks are immoral and that they run counter to the interests of the terrorists' potential supporters.

Seen in this light, it is clear that one or more successful attacks on American commercial aircraft would have profound strategic consequences for the United States and its partners in the fight against terrorist groups. America's enemies would gain a tremendous psychological boost from such attacks and would confront the world's population with serious doubts about not only the safety of air travel but also the viability of their governments' counterterrorism efforts. A new front would be opened in the contest and the effects would be long-lasting: in the popular imagination, the terrorists would be credited with having the capability to kill people on commercial aircraft more or less at will until such time as convincing policy solutions to the threat were implemented.

Of course, no countermeasure (or combination of countermeasures) can reduce to zero the possibility that terrorists could bring down an airliner with MANPADS. Less than perfect countermeasures have proven highly valuable in the context of military operations, where each aircraft is expected to encounter enemy defenses many times during its operational life span and where some risk of loss is accepted. The choice is less clear-cut in this case because the probability of an attack remains, by comparison, quite low, and because it is not clear whether the installation of less than perfect countermeasures will be sufficient to convince the vast majority of the public to return to flying.

The solutions we consider in this paper might render a MANPADS attack futile or even counterproductive. However, because of the complexity of technical countermeasures, it may take years before those solutions can be effectively designed and implemented. While that leaves open a window of vulnerability, waiting to start development until after an attack occurs would leave the defense of air travel that much farther behind. Thus, as we argue below, steps to develop them should proceed quickly.

Policy Solutions and Operational Issues

While this paper focuses on the question of countermeasures installation, there are other potential policy responses to the MANPADS threat that deserve mention. These responses are not mutually exclusive, but rather could act in concert to create a layered defense. As shown in Figure 5.1, the layers begin at the most distant remove by affecting the supply of terrorists and weapons (shown at the bottom of the figure) and range inward with increasing criticality to those that address post-incident crisis response (working to the top of the figure).

No individual solution will completely remedy the problem. Addressing it on a number of levels could decrease a potential attacker's confidence in the utility of MANPADS. The hope is that enough uncertainty about success will dissuade terrorists from choosing MANPADS as an attack means.

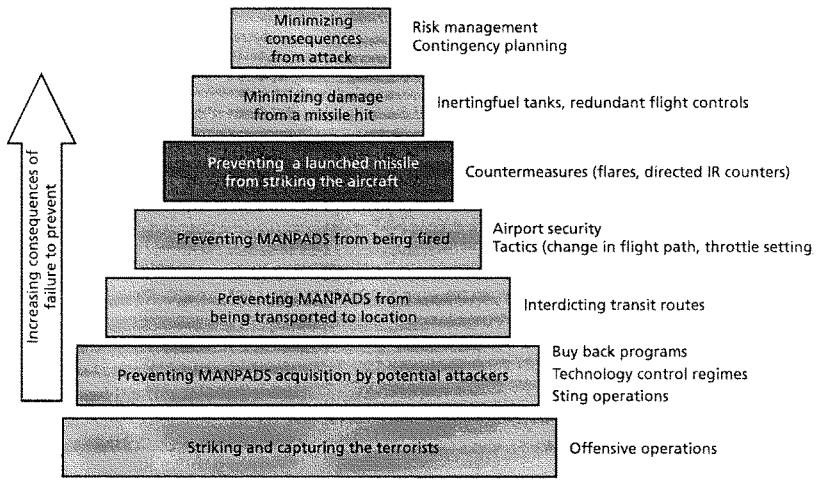
Taking the war to the terrorists' homeland seizes the initiative.¹ Offensive operations taken by the United States against terrorists where they are based (e.g., against al Qaeda in Afghanistan during Operation Enduring Freedom) is an important example. Striking and capturing terrorists not only affects the MANPADS threat but also other parts of the terrorist system. More focused options include buyback programs and technology-control regimes directed at MANPADS, which should help reduce current and future threat potential. To the extent that such initiatives do not keep MANPADS out of terrorist hands, there will be a need to improve security along borders and at transportation hubs to interdict the movement of people and weapons. Assuming these were not enough and that terrorists were still able to place MANPADS in the United States, we get to the final four layers of the solution space: preventing MANPADS from being fired, preventing a launched missile from hitting the aircraft, minimizing the damage from a missile hit, and minimizing consequences from an attack.

To prevent MANPADS from being fired, one could try to secure a perimeter around an airport that would prevent an attacker from firing from within range of the missile system. The range of a system like the SA-7 can extend out to 3.5 miles and a maximum altitude of 10,000 feet.² So where would the security perimeter need to extend to prevent a launch? To get a better sense of this, we need to consider the routes airliners fly when landing or taking off from an airport.

¹ We restrict ourselves here to security and military operations. We do not mean to slight the importance of fighting terrorism by addressing through political and economic means the conditions giving rise to it.

² Tony Cullen and Christopher F. Foss, eds., *Jane's Air Defense Systems, 2001–2002*, Surrey England: Jane's Information Group, 2001.

Figure 5.1
Protection Against MANPADS Provided at Many Levels



We were able to obtain, through public sources, standard arrival and departure patterns for Los Angeles International Airport (LAX). Noise regulations and other ordinances make these patterns available for many airports across the country. These patterns describe where and how low airliners fly in the airport's vicinity. With this information, we were able to define the area within which a terrorist armed with an SA-7 could pose a threat to an airliner. These findings are generally and broadly applicable to urban airports. We found that terrorists using that kind of MANPADS may engage aircraft while situated anywhere within an 870-square-mile area of the Los Angeles region. A more modern MANPADS (for example, the SA-18) has the capability to engage a slow-flying commercial aircraft up to 18,000 feet, which would allow the terrorist to be located anywhere within a 4,600-square-mile region. Against either the older or more modern threat, *completely* preventing an attack solely through the use of enhanced security perimeters would be impractical, considering the large urbanized areas involved, the cover provided by urban structures, and the availability of multiple freeways for quick access to attack and getaway (some of the flight paths extend over Santa Monica Bay, where a terrorist could engage an airplane from a small boat). However, since the probability that most MANPADS will hit a target drops rapidly when fired near their maximum range, the security emphasis might be placed on preventing launches from closer ranges—for example, near the airport. Secure perimeters close in could impede shorter-ranged threats of various types. As an example, a possible threat reaction to the installation of MANPADS countermeasures might be to use simpler weapons that are not affected by countermeasures, such as small arms or rocket-propelled grenades (RPGs) fired from a parking lot 100 feet under a runway approach.

In short, airport perimeter security is insufficient as a stand-alone defense against MANPADS but could serve as one of a number of layers in an overall suite of protection measures. In this context, it has the potential to blend in nicely with countermeasure-based solutions. Airport perimeter security also offers protection against other threats (e.g., the possibility of attacks on the airport itself).

If the layer attempting to prevent a missile launch fails, countermeasures might prevent the missile from making a successful hit. The basic types of countermeasures are discussed in more detail in the next section, but broadly speaking, different systems each have their own pros and cons. Some systems could provide highly effective protection under a wide range of conditions, but none are able to protect against the full range of threats. An understanding of where countermeasure weaknesses lie should help focus other counter-MANPADS policy efforts. As an example, if the countermeasures deployed are known to be marginally effective against a class of threat systems, buyback programs and nonproliferation efforts should pay particular attention to those systems. If we have an understanding of which types of aircraft are most vulnerable to MANPADS, this can help inform which aircraft should be fitted with countermeasures (or which should be fitted first).

By aircraft *vulnerability* to MANPADS, we mean the level of aircraft damage resulting when a missile strikes. Minimizing that damage is the next layer of defense. Vulnerability is an important consideration about which little is known in the case of airliners. There has been some renewed interest in the area, but at very low levels of funding.³ A good deal of research and testing has been done on the vulnerability of military transport aircraft, but these aircraft can be significantly different in design from commercial airliners: in many respects, military transports are designed to reduce their vulnerability to weapon fire. We do know that modern commercial airliners are designed and aircrews are trained to fly with one engine inoperable. MANPADS with infrared (IR) seekers are drawn to hot emissions or parts, such as those found on or near jet engines, so given the paucity of actual data, one might suppose that a MANPADS hit would at least disable an engine.

The aforementioned attack on the DHL aircraft departing from Baghdad International is instructive in this regard. Amateur video shows the missile type and launch geometry. This example suggests that the effects of a MANPADS hit can be more complex than the loss of an engine: in this case, it was reported that both engines of the aircraft were operable, but that all flight hydraulics were lost, primarily from fire-induced damage. There are technologies available that can help limit damage from fire, such as gas generator systems, which remove the highly flammable vapors in a fuel tank and replace them with a nonflammable inert gas. It would be expensive to retrofit these systems into existing airliners, however, and despite the DHL experience, the likelihood of extensive fire damage from a MANPADS hit is still unknown. Finally, as discussed above, the magnitude of the indirect losses from a successful MANPADS attack will depend on the ability of the authorities to reestablish the security of air travel and quickly convince travelers that they have done so. Contingency planning across law enforcement agencies could increase the probability that perpetrators are captured or killed.

³ See C. Pedriani, "JASPO/NASA Cooperate to Improve Commercial Aviation Security," in *Aircraft Survivability: Reclaiming the Low Altitude Battlespace*, Arlington, VA: Joint Aircraft Survivability Program Office, 2003.

Agreements may be reached in advance to implement various perimeter security measures that might be viewed as too costly or intrusive in the absence of an attack.

Planning and risk-management activities by officials not directly involved in law enforcement could also be helpful. For example, arrangements may be made in advance to alter aircraft approach and takeoff patterns in the event of a MANPADS attack. It will be essential that the messages the American public will be hearing from top homeland-security officials be consistent and accurately reflect the best knowledge available about risks. The large potential indirect losses we project are entirely due to actions taken out of perceived fear of attack. These losses can be reduced to the extent the fears are allayed. But if fears are falsely allayed—that is, if other attacks ensue following government assurances—the credibility of the government and its ability to manage risks could be severely damaged.

We here consider three major categories of countermeasures to MANPADS that are either deployed or under development: flares, laser jammers, and high-energy lasers (HELs). The first two aim to confuse the IR seeker of an infrared missile, while the HEL aims to destroy the missile, regardless of how it is guided. In this section, we discuss each in terms of basic operation, effectiveness, robustness *vis-à-vis* counter-countermeasures, and sensor support requirements. There are other potential countermeasures that will not be discussed, including defensive missiles (airborne or ground-based) and airborne lasers with sufficient power to destroy the seeker head. These will not be available in the near- to mid-term, and in any event do not appear to be well suited to civilian applications.

Flares

We describe three kinds of flares: conventional, advanced, and covert. *Conventional* flares were initially fielded to counter first- and second-generation passive IR missiles employing so-called seeker reticles: spokelike masks that rotate in the seeker's optical field of view and permit homing on the target. Conventional flares are intended to produce an IR signature so large that the target signature is overwhelmed, and the seeker locks onto the flare instead of the target. In quantitative terms, one speaks of achieving a high *jammer-to-target ratio* in order to capture the seeker.

Flares may be released either preemptively (before the onset of an attack) or reactively, after an IR surface-to-air missile (SAM) launch is detected. In a military setting, knowledge of when an aircraft enters a combat situation or arena can minimize the length of time that pre-emptive flares need to be released for. In the case of terrorists, such knowledge can be difficult to predict, and so for commercial applications, reactive flares are the practical consideration. In deployed systems, launch detection is usually accomplished by an optical or radar sensor onboard the aircraft; however, the cost-effectiveness of ground basing is receiving some scrutiny in recent studies. One drawback of ground-basing is the requirement for a highly reliable communications link from the sensor to the aircraft.

Seekers on some second- and third-generation IR SAMs are able to discriminate flares from aircraft due to the free-fall flight profile of the flare or its spatial extent, spectral properties, or intensity profile. As an example, modern two-color seekers can discriminate conventional flares from airplanes based on their spectral signatures (i.e., the relative signal strength in different wavebands, or colors). The ratios of intensities across different bands are indicative of temperature,

and flares are generally hotter than aircraft engines. *Advanced* flares can counter this discriminant because they consist of an ensemble (cocktail) of flares, each peaking in a different waveband, such that the combined signature matches that of the aircraft. Research is underway to replace cocktails with new single materials that can match target spectral signatures.

Some modern pseudoimaging seekers are able to discriminate against point targets such as flares by computing their aimpoint from the weighted centroid of the presented signature, including that of the airplane.¹ This discriminant can be negated by continuously dispensing advanced IR chaff, fabricated from pyrophoric materials, which react with atmospheric oxygen to release heat. Continuous dispensing can generate a chaff trail with sufficient extent to offset the centroid away from the target. The pyrophoric reaction is not sufficiently exothermic to render the material incandescent, so it is thought less likely that low-altitude release will cause fires on the ground than similar release of other flares. There is also no appreciable visible signature, leading to the common designation *covert*. Because of their covertness and reputed safety from fires, they are viewed as more suitable than other flares for installation on a commercial aircraft. The effectiveness of covert flares used in a *reactive* mode requires further development, however.

Flares, whether conventional or advanced, have little prospect for countering imaging seekers, which may be fielded by technologically advanced nations between 2005 and 2010. Flares are also ineffective against existing laser beam riders, which home in on a laser spot placed on the target by the SAM operator. SAMs that are radio-frequency (RF) command-guided (CG), like Blowpipe, are also largely immune to flares. The operation of such CG missiles is somewhat harder to employ effectively, since it requires users to keep the missile on an optical track between themselves and the target.

Since conventional flares could cause ground fires if released below about 1,000 feet, missile-warning system (MWS) used in conjunction with flares must generate few false alarms. Ultraviolet (UV) sensors, which are prone to false alarms, are thus not good candidates. Fusing multiple, independent phenomenologies (e.g., IR and Doppler radar sensors) have been proposed as a means to achieve an acceptable false-alarm rate. A Doppler radar measures the missile's radial velocity (i.e., its speed in the direction of the sensor). When viewed from the target aircraft, the missile's radial velocity shortly after launch is an unambiguous discriminant.

However, if a Doppler radar is deployed on the ground, it may face some delay before discriminating between SAMs and ground vehicles on a neighboring highway. Sensors looking normal to the missile's trajectory plane will initially measure zero Doppler, and seconds may be lost before the radial velocity exceeds the upper limit for vehicular traffic. This is particularly of concern if the aircraft is attacked at low altitude, which offers little time to respond. Employing steeper takeoff and landing profiles could be used to shrink the region susceptible to low altitude attacks, but the impact on safety of this option has not been fully evaluated. Providing geometric diversity by increasing the number of ground radars can ameliorate the problem, though at increased cost.

¹ Pseudoimaging seekers can coarsely resolve light sources within the field of view (FOV), either by scanning the FOV with a detector having a relatively small instantaneous FOV, or by employing a focal plane array (FPA) with a small number of detector elements. Some pseudoimagers also use two-color detectors to provide additional flare-rejection capability.

Key advantages of flares are that they are available today, they are fairly robust against even large salvos of older IR SAMs (which are the most highly proliferated), and they can be deployed based on detection of missile launch alone, not requiring sensors for tracking.

Laser Jammers

Laser jammers, which will soon be commercially available, are the most advanced form of directed infrared countermeasure (IRCM), or directed infrared countermeasure (DIRCM).² They will work best against first- and second-generation MANPADS. Their objectives are first to overwhelm the signal produced in the enemy missile's seeker by the target, and then to substitute a specially modulated signal³ transmitted by the laser, so as to divert the missile. The laser signal must emit at the color the seeker expects to see, be pointed with sufficient accuracy to enter the seeker optic, and achieve a large jammer-to-target ratio. Since the catalog of threats includes a variety of potential colors, a multiband laser or group of lasers is required for full protection. Laser spectra can be very narrow, but it is preferred that the DIRCM laser have a relatively broad spectrum to defeat narrowband optical filters that could be inserted in the seeker optic to block a jammer. Some DIRCMs employ optically pumped oscillators to jam the threat bands, and this technique typically results in broader spectra.

The laser modulation is designed to capture the seeker of a MANPADS and to break the seeker's lock on the targeted aircraft. In an *open-loop* system, the laser modulation is predetermined, so it must be designed to counter any of the likely threats. Open-loop DIRCMs have been developed by several contractors, and are in the testing phase. *Closed-loop* IRCMs (CLIRCMs), which are not yet available, are intended to capture retro-reflections from the seeker's reticle that can help to identify the attacking missile. The object is to focus all the laser energy in the appropriate passband and optimize the jamming modulation.

Laser-jammer systems are complex due to the need for highly accurate pointing. Satisfying this requirement demands that tracking sensors be mounted onboard the aircraft. Current practice is to also perform initial detection from the aircraft, although there are some potential advantages for locating this function on the ground. Following initial detection by an MWS, a fine tracking beam (e.g., a laser radar) is slewed towards the SAM, performs a limited search to acquire the missile, and then maintains a close track while the modulated laser illuminates the seeker. First-generation systems will employ turrets to slew the tracking and modulated beams. Eventually, this function may be performed by laser arrays, or micro electro-mechanical systems (MEMS) based optical elements. In the meantime, the turret is likely to be the most failure-prone component in the system.

² DIRCMs employing high-intensity lamps as sources have been deployed on aircraft in the past. They are inferior to laser jammers in several respects. The lamp is an incoherent light source and cannot deliver the small spot size, high intensity, narrow spectrum, and modulation flexibility of a coherent laser source. These deficiencies are elevated in importance when the aircraft signature is large, as with large commercial aircraft. Lamp-based jammers provide inadequate jammer-to-target ratio to confidently protect large jet-powered commercial airliners.

³ That is, the signal's variation over time in amplitude and frequency has been specifically designed to maximize its potential to confuse the enemy missile's seeker.

Stringent requirements for the MWS are high probability of detection and high accuracy. The tendency of the MWS to generate false alarms must also be taken into account, for three reasons. The first is that false alarms could lead to laser illumination of objects other than MANPADS and thus possibly to blinding of observers on the ground (this particular example would also require a false positive from the fine tracker). Laser eye-safe ranges for the DIRCMs being tested are on the order of several hundred feet. Because this is less than the minimum range of IR SAMs, the MWS could be set to ignore objects at such close range, which should rule out damage to the unaided eyes of persons on the ground. Evidence we have received to date concerning observers using binoculars appears contradictory. The second reason is that false alarms lead to slewing of the turret, which may ultimately shorten the time-to-maintenance or time-to-failure of this key component. The final reason is that false alarms could set off the contingency plans of local law enforcement, airport authorities, and airliners, which will limit their effectiveness during actual firings and accumulate in cost over time. There is no way to mitigate this problem, so minimization of false alarms will be an objective in MWS design.

Optical MWS sensors fielded thus far have typically operated in the UV "solar blind" region of the spectrum. This is the UV band in which upper atmospheric ozone almost completely absorbs solar radiation. In the absence of a missile plume, the sensor can be triggered by only a few manmade and natural sources, including high-intensity lamps, aircraft afterburners, corona discharges, and lightning. Unfortunately, these sources are not rare in urban areas.

Proposals for improving the MWS false alarm rates have included emplacing the UV sensors on the ground (false alarms looking skyward are presumably lower); adding a different phenomenology detector, such as a Doppler radar or one-color mid-wave IR (MWIR) sensor; or replacing the UV detector with a two-color MWIR detector. MWIR sensors employing large focal plane array (FPA) detectors are on the verge of supplanting UV MWS systems on the next generation of fighter aircraft, though MWIR false alarm rates remain a contentious subject. Manmade sources of MWIR false alarms are more numerous than UV sources, but the high resolution of FPAs may enable the MWIR sensors to kinematically discriminate the stationary sources.⁴ An important advantage of MWIR is its immunity to absorption by ozone in the lower atmosphere, which can be problematic for UV sensors in the urban environment.

In addition to false alarm rate issues, the sequence of events following initial detection by the MWS, which includes slewing of the turret, fine tracking, and then a dwell period to break the seeker's lock, requires that the turret focus on one threat at a time. The DIRCM has some limitations against multiple threats, and though one could equip an aircraft with multiple turrets to increase the number of near-coincident launches that can be defended, this would obviously increase installation and operating costs by nearly that multiple.

As with flares, laser DIRCMs are not effective against laser beam riders (for which they may only furnish a beacon), RF CG missiles, and future imaging IR seekers. Current research is exploring whether IR focal planes might be disabled or degraded with increased laser power, but this is speculative and represents a departure from the basic DIRCM concept.

⁴ That is, use the motion of different objects relative to the airborne MWIR to determine which are actually stationary on the ground.

To sum, a single-turreted laser-based countermeasure system would have good effectiveness against single shots by the majority of current MANPADS threat types and some dual coordinated firings but would not fully protect against all possible attacks.

High-Energy Lasers

It was recently reported in the press that Northrop Grumman's ground-based mobile tactical high-energy laser (MTHEL) test-bed has destroyed artillery shells and Katyusha rockets in flight. The rocket is almost certainly a more hardened target than a SAM, which suggests that high-energy lasers might be used to protect commercial aircraft from shoulder-fired missiles in the vicinity of airports.

A palletized variant⁵ of MTHEL, called Hornet, has been proposed for a wholly ground-based defense against MANPADS. The Hornet system would include a radar air picture to designate vectors along which the laser could not fire because friendly air traffic might be in the line of sight; netted IR search-and-track (IRST) systems for acquiring and tracking SAMs,⁶ and for pointing the laser; and a megawatt-class deuterium fluoride chemical laser weapon housed in a turret on the ground.

Advertised performance of a single Hornet site indicates capability to defend against salvos of three missiles out to a range of at least five kilometers, with single-missile protection out to ten kilometers.⁷ Robust protection of a large airport such as Reagan National would require a minimum of three sites. This assumes flight-corridor adjustments to keep aircraft above the SAM ceiling except when required for landing and takeoff. Many more would be required without corridor adjustments.

The primary advantages of HELs for SAM defense are the ability to counter every current and future seeker technology, the robustness of a lethal kill as compared to smart jamming of the seeker, and the potential for defending against a wide variety of threats, including artillery, rockets, some cruise missiles, and hostile unmanned aerial vehicles (UAVs). HELs cannot operate under all weather conditions. Conditions that render the HEL inoperative will usually deny capability to MANPADS as well, but this is not true all the time. A spatially inhomogeneous fog layer may occasionally shut down the laser while leaving an open patch in which the SAMs can launch. At such times, unprotected flight corridors would have to be closed if no window of opportunity is to be left for MANPADS attack.

Eye safety is a concern when firing high-powered lasers, even if the lasers operate in the eye-safe band, as do deuterium fluoride lasers. Eye damage could arise either due to direct illumination of a person in an aircraft, or secondarily when persons in aircraft or on the ground see the destruction of the missile. The former problem should largely be circumvented by using the radar

⁵ That is, one packaged for installation aboard a vehicle.

⁶ Including initial detection sensors onboard the aircraft would not be incompatible with the Hornet concept and might improve response time in built-up areas.

⁷ Fewer missiles can be destroyed at greater distances because the dwell times have to be longer to compensate for the dissipation of energy.

air picture to set up keep-out zones for the laser. There may be a rare occasion when untracked aircraft are illuminated, because air-traffic control radars do not detect with absolute certainty. However, since the laser beam must be slewed rapidly to keep pointed on the missile, any chance illuminations would last only milliseconds and would not cause damage. Diffuse reflections coming off the missile while it is illuminated can reach damage-level intensity only at a range of a few meters, which is clearly avoidable.

Perhaps the major drawback for HEL technology is availability. Estimates are that the start of production is at least three years away. This compares with current or imminent production for advanced flares, and for DIRCMs, though the latter's production *rate* may still be at issue.

Another concern with all the countermeasure systems discussed involves technology sharing and classification issues. Laser jam codes, sensor processing algorithms, and HEL systems are all sensitive technologies, which would need to be guarded. Assuming U.S. airliners would need to be protected during overseas flights (which many argue are the most vulnerable to terrorist attack), the question is how to maintain the systems and guard their classified information while in a foreign commercial-airport environment. This would particularly be troublesome for ground-based defenses such as the HEL system.

Figure 6.1 summarizes the effectiveness of flares, laser jammers, and HELs against different threat types.

Figure 6.1
Summary of Potential Counters to MANPADS

Threat type	Proliferation	Countermeasures			High Power Laser
		Flares	Laser		
Older generation infrared (IR)		Very wide			
Current generation IR		Wide			
Radio Control		Limited			
Laser Beam Rider		Limited			
Future IR (imagers)		None			

 Demonstrated
  Limited
  No Effectiveness
  Potential

RAND OP106-2.2

In this section, we estimate the cost of one class of MANPADS countermeasure described earlier: the laser-based DIRCM. Flares have the potential to be a cheaper alternative to laser jammers, but their effectiveness in a commercial-airliner application has more question marks. Ground-based HEL systems have excellent potential against current and future threats, including non-IR-based threats, but are not as far along as the laser-based DIRCM. It follows that remaining development costs in a commercial-airliner application would be more lengthy and expensive, although the overall *system* benefits may outweigh these initial costs. Even for aircraft with large IR signatures, laser jammers promise substantial capability against first- and second-generation MANPADS systems, due to the high signal-to-target ratio provided by the focused energy of the laser. From a technical-maturity standpoint, significant testing and development of this class of system have been done for the military (including live-fire tests in realistic conditions). It is therefore a front-runner for consideration of any kind of fast-paced near-term countermeasures installation program for commercial airliners. Though we restrict our specific cost estimates to DIRCMs, some of the cost issues highlighted in this section are relevant to the installation of other countermeasure types.

Total life-cycle cost (LCC) estimates can be broken down into two categories: installation costs and operating and support (O&S) costs. The LCC estimates are summarized in Table 7.1 for a projected quantity of 6,800 U.S. commercial aircraft. We examine estimates for these two cost categories in further detail below, and then conclude by considering total program costs in the context of the federal counterterrorism budget.

Installation Costs

We made “first cut” cost estimates for installing the most promising near-term airborne DIRCM systems on the fiscal year (FY) 2003 inventory of approximately 6,800 U.S. commercial aircraft.¹ These costs were based on modifying the most current set of parametric cost data values from technically analogous military systems, such as the Air Mobility Command’s large-aircraft IRCM (LAIRCM) system.² Specifically, we adjusted weights and volumes calculated

¹ The FY 2003 U.S. Aviation Inventory forecast was extracted from B. Turner, “FAA Aerospace Forecasts, Fiscal Years 2003–2014,” February 13, 2003, Table I-2.

² RDT&E and procurement budget data on two Air Force programs, the laser-based LAIRCM system and the Special Operations Force’s (SOF) AN/AAQ24 (V) 6 (lamp-based) DIRCM system, were extracted from the “FY-2004/2005 President’s

Table 7.1
Total Airborne DIRCM System LCC Estimates (FY 2003 dollars, billions)

Cost Element	Estimate (FY-2003 B\$)
Installation	\$11.2
• RDT&E	\$0.45
• Production Start-Up	\$0.17
• Initial Spares and Test Benches	\$0.90
• A & B-Kit Procurement & Aircraft Retrofit (Based on Qty of 6,800)	\$9.75
• O&S (Phase-In and Ten-year Service Life After FOC)*	\$27.0
• A & B-Kit Maintenance	\$12.5
• Added Fuel	\$4.2
• Cost Growth/Uncertainty (25 Percent)	\$4.2
• Tech Upgrade Sustainment Cost	\$4.1
• Net Revenue Loss of Delayed Passengers	\$2.0
Total LCC Estimate	\$38.2

* If an RDT&E phase begins in FY 2004, the first year of procuring DIRCM-modification kits for retrofitting commercial aircraft is assumed to begin in the FY 2007 time frame. Phase-in of O&S costs for the first configured aircraft begins in this fiscal year and continues until the last commercial aircraft is retrofitted in FY 2013. O&S cost continues once full operational capability (FOC) of all aircraft is completed in FY 2014, and costs are estimated annually for a ten-year service life through FY 2023.

for the military version to meet the form and fit required to enclose all the electronics within a canoe-shaped pod installed on the underside of commercial aircraft.³ The airborne DIRCM systems proposed for commercial aircraft comprise

- an MWS of four two-color MWIR sensors capable of detecting a MANPADS approaching within the full range of velocities and angles possible
- a system processor designed to military specifications using fifth-generation or better central processing unit electronics along with a smart jamming card
- an electronic control unit that conditions the power and signals for the laser transmitter
- a multiband laser transmitter mounted within a small turret
- a command, control, and communications system to provide missile warning updates and intercept data to ground control operations
- a built-in-test hardware and software subsystem
- the canoe-type surface mounting hardware package and other A-kit interface hardware to enclose the preceding system components⁴

We estimate a total fleet installation cost of \$11.2 billion.⁵ That includes the

Budget Item Justification" sheets, February 2003. In addition, installation plans were outlined for the latter SOF DIRCM system as part of J. Townsend, "15 SOS Field Support Visit Aircraft Modernization," unclassified briefing, HQ AFSOC/XPQA, Halbur AFB, January 23, 2001.

³ The parametric cost data and procurement estimates were based on the Navy's tactical aircraft DIRCM system data that was part of M. Popp, "Cost Analysis Update," briefing to the Interagency Task Force, NAVAIR 4.2V, Washington, D.C. February 13, 2003.

⁴ A-kits are defined as the aircraft installation equipment used to attach and complete any wiring of the countermeasures to an airframe. B-kits are defined as the actual countermeasures equipment without installation.

⁵ All costs in this section are given in FY 2003 dollars.

- research, development, test, and evaluation (RDT&E) phase at \$445 million, consisting of the systems design, aircraft flight testing, and Federal Aviation Administration (FAA) certification⁶ for six fully configured prototype systems
- manufacturing technology, capital, and facilities costs at \$165 million to build up the annual production rate needed through the end of low-rate initial production (LRIP) (\$65 million), and the set-up tooling of a second final assembly and test manufacturing line for the entire full-rate production (FRP) phase (\$100 million)
- purchase of initial spares and test bench equipment at \$900 million
- procurement and retrofit of approximately 6,800 DIRCM B-kits and A-kits at \$9.75 billion

We assumed the development phase of a commercial DIRCM system begins in FY 2004 with the first year of RDT&E annual funding for the program office and continues for four years, until the end of FY 2007. The development estimate assumed the six flight-test prototypes would be adequate for integrating and checking out all the structural, electrical, and other interfaces required across the most representative subset of commercial aircraft models. In addition, the estimate includes a sufficient number of prototype ground and flight tests to ensure that the acoustic, vibration, and other environmental conditions of each aircraft model are within acceptable limits for the system to operate effectively. Finally, the total RDT&E estimate includes an adequate number of reliability and maintainability demonstrations within commercially acceptable threshold and objective values, especially for the on-equipment maintenance turnaround times across each of the different commercial aircraft models (as explained below, these could affect O&S costs if the targets are not met). To allow for these activities, we estimated the commercial DIRCM system development cost by increasing the LAIRCM RDT&E total budget by 60 percent (i.e., another 1.6 times the LAIRCM budget will have to be spent to fund DIRCM RDT&E for commercial aircraft). That factor was based on the following considerations:

- extent of repackaging of the B-kits to fit within the canoe structure
- number of unique A-kit designs needed for each commercial aircraft model
- number of flight tests required for installing, testing, and certifying the systems on all the commercial aircraft models

Procurement is projected to begin with an LRIP phase starting in FY 2006 during the third year of the system development phase and continuing through FY 2009. By then, approximately 1,100 commercial aircraft would be fitted, enough to cover all three stages of civil reserve airfleet (CRAF) deployment,⁷ as well as all long-haul large jets for international and domestic flights. FRP will cover the remainder of the civil aviation fleet and will start immediately after the end of LRIP in FY 2009 and proceed through FY 2013. The cumulative average unit

⁶ The FAA would be required to issue Supplemental Type Certificates that have demonstrated that DIRCM systems are capable of operating without conflicts or problems.

⁷ Even though only a handful of designated commercial aircraft may have been deployed to support the last several conflicts in Iraq and Afghanistan, the U.S. Transportation Command, with approval of the Secretary of Defense, has authorized quantities of commercial aircraft that can be activated for all three stages of CRAF. The quantity of CRAF aircraft over the three stages is listed as part of Air Transport Association, Office of Economics, June 21, 2003, <http://www.airlines.org/econ/p.aspx?nid=6342> (as of November 3, 2003).

production cost (AUPC) is estimated at \$1.3 million (in FY 2003 dollars). This cumulative AUPC is the sum of the unit cost of the following:

- airborne DIRCM system A-kit, B-kit, and system installation cost
- the cost of the initial spares, technical data, support equipment, and change orders, amortized on a per-system basis by applying a 92 percent cost improvement curve or learning curve slope⁸ across the total quantity of approximately 6,800 systems.

Operating and Support Costs

We estimated an annual O&S cost per aircraft of \$300,000 for a subtotal O&S cost of \$27 billion through FY 2023. These costs consisted of the following:

- added fuel cost (of \$45,000 per aircraft per year) needed due to the drag and additional weight that the commercial aircraft will be carrying over an assumed 3,000 hours per year
- maintenance cost (of \$140,000 per aircraft per year) of the
 - airline mechanics labor, spares (following the initial buy), and other material needed to do on-equipment airport ground maintenance
 - airline depot-level or contractor logistics support activities for scheduled system overhauls and repairs and for unscheduled repairs of failed components sent back from the airport
- technology upgrade sustainment costs (of \$60,000 per aircraft per year) that maintain the capability of the countermeasures as different threats emerge (however, this would not account for dramatic shifts in threat capability)
- operations costs due to airplane delays (of \$15,000 per aircraft per year)

The added fuel cost estimate is based on an increased drag estimated at 0.4 percent and an added system-level total weight (including a 25 percent margin) of approximately 500 lbs. divided between the following:

- B-kit estimated weight of 125 lbs.
- weight of the canoe and other A-kit hardware (airframe structural material, wiring, doublers, isolators, etc.) estimated at 375 lbs.⁹

The maintenance cost estimates were driven by

- a mean-time-between-failure (MTBF) estimate of 800 hours, based on projected military-system reliability

⁸ That is, each doubling in production quantity results in an 8 percent unit cost decrease.

⁹ The B-kit and A-kit weight estimates are based on weights provided for comparable military systems (from Popp, 2003) adjusted to fit within the volumetric constraints on the underside of a representative commercial aircraft.

- an assumed duty cycle of 55 percent based on the system being on for only 30 minutes during takeoff and 30 minutes during landing for all short-haul and long-haul (international and domestic) commercial aircraft
- a built-in-test or health monitoring subsystem sufficient in capability to reduce the elapsed turnaround time for on-equipment (airport) maintenance to 30 minutes or less for short-haul flights and between two and four hours for long-haul international or domestic flights
- finally, another 25 percent added to the maintenance and delay costs (\$40,000 per aircraft per year) to account for the cost growth uncertainty in the estimates, since there is only limited field experience from which to infer O&S costs, and that is with a military DIRCM system based on a lamp, not a laser; the assumed 800-hour MTBF is the reliability derived from the most analogous LAIRCM system, which is based on lower-level hardware estimates

The total O&S cost is thus \$27 billion. Once all systems are installed, annual O&S costs would amount to a little over \$300,000 per airplane, or \$2.1 billion for a 6,800-plane fleet.

Two O&S cost-related issues could add to the overall uncertainty and potential cost growth of the LCC estimates. First, how would passenger flight safety concerns related to a faulty airborne DIRCM system affect the airline industry's record for on-time departures, if the countermeasure system were considered flight-critical hardware? What will be the criteria by which airline mechanics and airport schedulers decide it is prudent to delay scheduled departures? Decisions for this system are more comparable to a breach or malfunction in the security doors of the pilot's cockpit as opposed to detecting an oil leak coming from one of the engines. Second, our LCC estimates are based on designing and producing robust, highly reliable systems that will allow for on-equipment airport turnaround times fast enough to fit within most of today's flight schedules. MTBFs that exceed our assumed values or failure of the built-in test system to allow rapid enough diagnostics could lead to

- procuring higher quantities of spares (initially and annually) to supply airport maintenance activities
- late departures or flight cancellations, as noted above

Our uncertainty allowance may cover the first of these consequences, but it was not intended to encompass the second. The costs of late departures could be substantial. For example, suppose all detected DIRCM system failures take more than 30 minutes to fix for short-haul flights, and 75 percent of them take more than four hours for long-haul flights. If the net revenue loss for each hour of delayed departure is \$10,000, the annual O&S cost would increase by 18 percent, from \$2.1 billion to \$2.5 billion. To avoid such losses, airlines may choose to increase the use of available aircraft at airports or activate reserve aircraft to fill in, but these options have their own costs.

One of the goals of a countermeasures development program would be to increase the reliability of such systems in order to reduce the O&S costs.¹⁰ We examined the impact of in-

¹⁰ See S. Erwin, "Anti-Missile Program for Airliners on a Fast Track," *National Defense*, December 2003, <http://www.nationaldefensemagazine.org/article.cfm?Id=1281> (as of February 1, 2004).

creasing the MTBF of countermeasure systems to 3,000 hours (vice 800). Annual O&S costs fell from \$2.1 billion to \$0.9 billion, and ten-year LCCs fell from \$38 billion to \$25 billion, so there is a significant potential payoff involved in increasing the installation costs from \$11.2 billion to \$13.4 billion for designing and procuring a more reliable system.

There is one further element we have not included. Even though the commercial DIRCM system will be designed to operate autonomously and not require pilot intervention, it will need to include communications links for transmitting data directly to law enforcement, transportation security, aviation safety, and homeland-security authorities located at ground command and control (C²) centers. In other words, it needs to be able to integrate into an overall aviation safety and security *system*. The purpose of this link into the system is threefold. First, the link would serve to pass system reliability information on to aviation security officials. This would inform flight procedures if countermeasure systems break down prior to takeoff or during flight. Second, the link should inform aviation safety officials when MANPADS-related events are being detected so as to notify nearby aviation traffic of possible danger. Third, the link should inform law enforcement authorities by indicating the nature of the attack and the estimated location(s) of attackers. It should be noted that the latter two could include false alarms, so procedures need to properly balance security, safety, and economic issues. Even though the cost of this communications link is included in the installation cost estimate, the entire *system* concept of operations should be articulated clearly prior to finalizing system design and before starting LRIP. In addition, the cost of the infrastructure, staff, and equipment for ground-based C² centers would have to be added to the total LCC estimate as part of the overall systems architecture.

Even if the total development, procurement, and installation costs, estimated at \$11 billion, were fully borne by the federal government, this expense covers only 29 percent of the total LCC of \$38 billion. There is no guarantee that the government will pay all or any of the \$27 billion costs of operating and supporting the airborne DIRCM systems from FY 2007 through FY 2023. Even in the highly competitive environment of the U.S. commercial-airline industry, this additional O&S expense and potential loss of revenue can only be made up through increasing passenger ticket prices.

Given the magnitude of the uncertainty described above and other related factors that are projected to drive maintenance costs, while the O&S cost could certainly increase, improved reliability of the system would reduce these costs by a factor of two or more. Therefore, one of the primary objectives of any countermeasure development and evaluation effort should be to reduce those uncertainties.

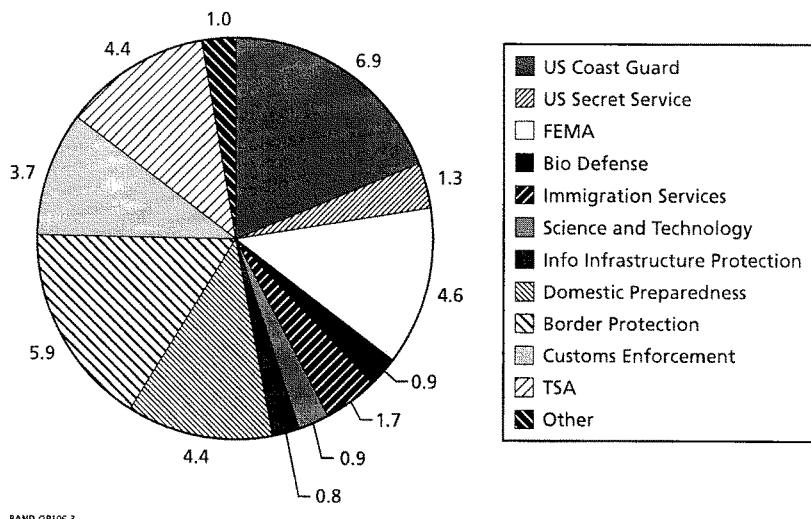
Budgetary Considerations

Clearly, MANPADS countermeasure implementation will be costly. While the potential economic and strategic costs stemming from an attack could be even greater, allocation of resources to countermeasures may mean a reduction in resources applied to other parts of aviation security, as well as to other homeland-security and counterterrorism efforts. More broadly, resource allocation for protecting commercial airliners should strive to be based upon risk, vulnerability, cost, and benefit. They would weigh the risk from a variety of attacks, such as MANPADS, bombs, small arms, and RPGs and then compare side by side the cost and benefits of various counters, such as IRCMs, bomb-resistant containers, and airport security procedures.

Any decision about government-mandated countermeasures installation aboard commercial airliners should thus consider the overall budget available (or necessary) for homeland-security purposes and the more general struggle against terrorism. The FY 2004 Department of Homeland Security (DHS) budget is \$36.5 billion. In the broader struggle against terrorism, the President's budget request for FY 2004 included \$16 billion for military operations and recovery efforts in Afghanistan and \$71 billion for Iraq.¹¹ In comparison to these figures, the anticipated \$2.1 billion annual O&S cost for MANPADS countermeasures seems small. However, as indicated by the DHS budget breakdown in Figure 7.1, \$2.1 billion is a substantial fraction (almost half) of the resources being devoted to all of transportation security in the United States today (the pie slice labeled *TSA*). And countermeasures against MANPADS are only one layer of responses against one of many possible threats to air travel.

We should note that our cost estimates encompass only the period through 2023. At that point or even earlier, it may become desirable to replace the laser-jammer systems with HELs, if more sophisticated MANPADS proliferate among terrorists. In contrast to the next several years, in which countermeasure installation can begin with no preexisting O&S demand, the installation costs of future countermeasure generations could lead to total amortized program costs well in excess of the annual O&S figure we cite here.

Figure 7.1
FY 2004 Expenditures for DHS (billions of dollars)



¹¹ Data for homeland-security expenditure comes from Department of Homeland Security, "FY2004 Budget Fact Sheet," <http://www.dhs.gov/dhspublic/display?content=1817> (as of October 2003). The spending estimate for the military and reconstruction efforts in Afghanistan and Iraq come from the President's FY 2004 supplemental appropriations budget request.

Summary and Recommendations

Air travel has become an integral part of modern life. Terrorists have long understood this and have made commercial aviation one of their prime targets. Al Qaeda and its affiliates have both the motive and the means to bring down U.S. commercial aircraft with MANPADS. No such attempt has yet been made against a U.S. carrier, but given the measures being taken to preclude 9/11-style attacks, the use of MANPADS will unavoidably become more attractive to terrorists.

What might be done to prevent such an attack? We concentrate here on the capabilities and costs of onboard technologies to divert or destroy an attacking missile. Given the significant costs involved with operating countermeasures based upon current technology, we believe a decision to install such systems aboard commercial airliners should be postponed until the technologies can be developed and shown to be more compatible in a commercial environment. This development effort should proceed as rapidly as possible. Concurrently, a development effort should begin immediately that focuses on understanding damage mechanisms and the likelihood of catastrophic damage to airliners from MANPADS and other forms of man-portable weapons. Findings from the two development programs should inform a decision on the number of aircraft that should be equipped with countermeasures (from none to all 6,800 U.S. jet-powered airliners) and the sequence in which aircraft are to be protected.

If it is determined that U.S. commercial airliners should be equipped with countermeasures upon completion of the development program, they should be employed as part of a broader set of initiatives aimed at striking and capturing terrorists abroad, impeding their acquisition of missiles, and preventing them and their weapons from entering the United States. Attention should also be paid to keeping MANPADS-equipped terrorists out of areas adjacent to airports and improving commercial airliners' ability to survive fire-induced MANPADS damage.

A multilayered approach is important because no single countermeasure technology can defeat all possible MANPADS attacks with high confidence. Nonetheless, substantial protection can be achieved. Laser jammers, for instance, will be commercially available for installation aboard airliners soon and should be able to divert single or possibly dual attacks by the relatively unsophisticated MANPADS accounting for most of those now in the hands of terrorists. Ground-based HELs intended to destroy approaching missiles could counter MANPADS of any degree of sophistication, but they are not ready for deployment in the next few years and have significant operational challenges to overcome. Pyrophoric flares used reactively offer the promise of a cheaper alternative with better potential to handle multiple attacks than laser-based systems, but their effectiveness at protecting large transport aircraft from any

MANPADS attack is not well established, and they would be most likely ineffective against sophisticated future systems.

We estimate that it would cost about \$11 billion to install a single laser jammer on each of the 6,800 commercial aircraft in the U.S. fleet. The operating costs of fleetwide countermeasures will depend on the reliability of the system. Extrapolating from early reliability data from the systems currently deployed on large military aircraft, the O&S costs for a commercial variant were assessed to be \$2.1 billion per year for the entire commercial fleet. The full ten-year LCCs for developing, installing, operating, and supporting laser-jammer countermeasures are estimated to be \$40 billion. If reliability goals recommended by DHS can be achieved, the ten-year LCCs are estimated to be \$25 billion.

When would such an investment be worth it? That is not a question answerable solely through quantitative analysis, but some light can be shed by four avenues of inquiry. First, what would be the likely economic costs of a successful attack? If we take into account the value of a lost aircraft and a conventional economic valuation of loss of life, the *direct* cost would approach \$1 billion for every aircraft downed. The indirect economic damage from an attack would be far greater. These costs result from the loss of consumer welfare through preemption of a favored travel mode or reluctance to use it, as well as operating losses suffered by airlines subsequent to an attack. These amounts will depend primarily upon two factors: the length of any possible systemwide shutdowns in air travel and any kind of longer-lasting public reluctance to fly. Both factors are difficult to predict, but if air travel were shut down for a week (it was shut down for three days after 9/11), the economic loss would amount to roughly \$3 billion during the shutdown itself. Extrapolating from the long-term effects of the 9/11 shutdown, losses over the following months might tally an additional \$12 billion, for a total economic impact of more than \$15 billion.

A second avenue of inquiry can help place the cost of MANPADS countermeasures in context. To what extent must homeland-security and other counterterrorism resources be expanded or diverted to fund this one effort to help respond to a single threat? The \$2.1 billion annual O&S cost, should it be borne by the government, amounts to only about 6 percent of the annual DHS budget. The fraction is much smaller if the costs of operations in Iraq and Afghanistan are included in the base. However, the \$2.1 billion is a substantial fraction of total current federal expenditures on transportation security.

Third, it must be recognized that loss of life and economic impact would not be the only costs of a MANPADS attack. The perceived inability of the U.S. government to prevent attacks on its citizens on its own soil would set back U.S. efforts to counter terrorist groups globally and could weaken U.S. influence across a range of other interests abroad. Such an attack would also cause unquantifiable losses of security among the U.S. populace.

Fourth, and lastly, while countermeasures have been demonstrated to be an effective resource in protecting our military aircraft, the circumstances of protecting commercial airliners from terrorists are sufficiently different that we should ask ourselves the following questions: Upon deployment of countermeasures, how easy do we think it will be for terrorists to adapt and find vulnerabilities to airliners through the use of weapons that are not affected by countermeasures? Would defenses against these weapons be possible, or would they require a similar level of funding to protect against?

A decision as to whether to proceed with a MANPADS countermeasure program must thus balance a variety of considerations. On the plus side:

- New countermeasure technology with capability against a variety of attack situations will be available in the near term, with the potential to avert the loss of hundreds or even thousands of lives and tens of billions of dollars.
- Funding such a system would require a reallocation or expansion of federal homeland-security resources of perhaps 5 percent—and a much smaller proportion of total federal counterterrorism resources.

On the minus side:

- Annual operating costs would represent nearly 50 percent of what the federal government currently spends for all transportation security in the United States.
- Well-financed terrorists will likely always be able to devise a MANPADS attack scenario that will defeat whatever countermeasures have been installed, although countermeasures can make such attacks considerably more difficult and less frequent.
- Installing countermeasures to MANPADS attacks may simply divert terrorist efforts to less protected opportunities for attack. To put it another way, how many avenues for terrorist attack are there, and can the United States afford to block them all?

Given the significant uncertainties in the cost of countermeasures and their effectiveness in reducing our overall vulnerability to catastrophic airliner damage, a decision to install should be postponed, and concurrent development efforts focused on reducing these uncertainties should proceed as rapidly as possible. The current DHS RDT&E activities are a prudent step both toward reducing significant cost uncertainties involved and minimizing the delay of program implementation once a go-ahead decision is reached.

To summarize, any federal policy to protect against MANPADS should not be restricted to countermeasures development but should involve multiple layers, with emphasis on the following areas:

1. Rapidly understanding and finding ways to reduce the O&S cost component of countermeasures in a commercial-airline setting. In addition, decisionmakers should be thinking about how specific countermeasure systems would work best in conjunction with other protection efforts and technologies. Understanding the weaknesses of countermeasures should help focus these efforts, and vice versa.
2. Focusing a concurrent technology development effort on understanding damage mechanisms and the likelihood of catastrophic damage to airliners from MANPADS and other forms of man-portable weapons such as RPGs, mortars, and small-arms fire. This will serve three purposes: clarifying the damage caused by single or multiple MANPADS hits on airliners, informing choices regarding the implementation of mitigating measures such as inerting fuel tanks and missile countermeasure systems, and assessing the seriousness of other forms of attack against airliners.

3. Working with international governments to slow down the proliferation of MANPADS technologies, in particular those against which countermeasures are less effective.
4. Putting together concepts of operation that integrate countermeasures into the overall aviation safety, security, and law enforcement system. These can help local law enforcement establish the size and location of airport security perimeters and define ways in which information from the onboard countermeasure system sensors can be used to help find, track, and apprehend MANPADS operators. Lastly, they would help provide an understanding of the costs from false alarms to air-traffic operations and local law enforcement.

APPENDIX A

Estimating Consumer Surplus Loss

To estimate the actual consumer surplus for a successful shoot-down of a commercial aircraft in the United States, we first divide air travel into different market segments based on length of trip. Then we estimate the cost of travel for different travel modes, including air travel and its alternatives, in these market segments. We examine travelers' willingness to pay to avoid the shutdown of air travel, which varies by segment, and calculate the consumer surplus loss that results.

Segmenting the market. Table A.1 provides an estimate of the number of household trips taken by commercial airplane—an estimate that is used to calculate the percentage share of air-traveler miles according to the round-trip distance traveled for each trip. These trips are sorted into five different distance categories. An average number of miles flown is taken for each distance category and multiplied by the number of trips to generate the number of miles flown for each distance. This calculation generates the distribution of miles among different trip distances, which will be used in later calculations. The vast majority of airline passenger miles occurs during long trips—those at least 1,000 miles in each direction.

We break the market for air travel down further according to trip purpose (business or leisure) and destination (domestic or international). Business and leisure travelers tend to make different decisions about the speed and cost of transportation, and they tend to value time differently. On average, half of airline travel tends to be business and the other half leisure. Domestic and international travel is split because relatively convenient alternatives exist for domestic flights, while without air travel international trips to any place outside of Canada and Mexico become highly difficult. For Americans, about three-quarters of air mileage is domestic, and the rest international.

Estimating the costs of alternatives. In the case of an air-travel shutdown, travelers would need to take a car, train, or bus to reach their destination; some travel would undoubtedly be canceled. More than 90 percent of all non-air trips, even at the longest distances, are taken by car. Furthermore, transportation-mode-choice models of intercity travel generally show bus travel to have a specific disutility associated with it that cannot be easily attributed to its cost or its speed.¹ That is, many travelers exhibit distaste for bus travel that cannot be readily translated to the kind of welfare calculations we are going to make. Therefore, we will consider car and train as the two alternatives when air travel is disrupted.

We next estimate the change in trip cost that would occur when switching from flying to using an alternative mode. For international travel outside of North America, which means

¹ For example, see Steven A. Morrison and Clifford Winston, "An Econometric Analysis of the Demand for Intercity Passenger Transportation," *Research in Transportation Economics*, Vol. 2, 1985, pp. 213–37.

Table A.1
Aviation Miles by Trip Distance

Round Trip Distance	Average Round Trip Distance	Commercial Aviation Trips (thousands)	Commercial Aviation Miles (thousands)	Percent of Total Miles
<300 miles	250	1,364	341,000	0.1%
300-499	425	7,118	3,025,150	1.1%
500-999	800	26,812	21,449,600	7.9%
1,000-1,999	1600	36,294	58,070,400	21.4%
>2,000 miles	3525	53,295	187,862,362	69.4%

Source: USDOT (1997)

most international flights, no viable alternative mode exists. For domestic trips, we calculate the time and cost involved for each of the three modes: air, car, and rail, for each average round-trip distance (see Table A.2). Travel times are calculated based on travel speeds. The trip distance is divided by the average speed of each mode to generate a trip time in hours. Two additions are made to these travel-time calculations. For air travel, time is added for travel to and from the airport and for the time required for check-in and security screening. For car travel, allowance needs to be made for trips that would last longer than a normal driving day. To translate trip times to dollar values, we use estimates of the value of travel time for business and leisure travelers. The value of time for leisure travelers is taken as \$19.50 per hour, and the value of time for business travelers is given as \$34.50 per hour, per FAA guidance.²

Cost data for air travel comes from the Air Transport Association (<http://www.airlines.org/>). Passenger yields in 2001 for domestic air travel averaged 13.4 cents per mile. Since exact cost data are not available for passenger operations separate from cargo operations, we assume that per-passenger revenues are approximately equal to per-passenger costs. Auto-travel costs are calculated by the consulting firm of Runzheimer International and are available at their Web site (<http://www.runzheimer.com/>). The full costs of owning and operating an automobile were calculated at 52 cents per mile. However, on average most auto users do not travel alone. Therefore, we assume that two people take the average auto trip and thus figure the cost at 26 cents per mile. Rail-travel costs come from the Amtrak Annual Report. The 25.7 cents per-mile cost used here is for a seat mile of travel.

When time and travel costs are added, we find that for trips of 800 miles and less, the sum is lower for car travel than for train travel. However, train travel is less costly than car travel for trips in the longest two distance categories. This holds true for both business and leisure travel. The combined cost difference between air travel and the best alternative is calculated and expressed as both a percentage change and a per-mile difference; this is then used in calculating the change in consumer welfare.

Calculating consumer surplus. To estimate consumer surplus, we need to know the difference between consumer willingness to pay and price. For this study, we approximate the willingness to pay for air travel by using the elasticity of demand. The elasticity of demand describes the percentage change in demand for air travel given a percentage change in its price.

² FAA, 1998.

Table A.2
Travel Costs for Air and Alternative Modes

Leisure Travel					
Airline	Cost per mile: \$0.134	Time cost: \$19.50	Avg. Speed: 400		
	Trip Length	Time (hours)	Time Cost	Travel Cost	Total Cost
	250	6.63	\$129	\$34	\$163
	425	7.06	\$138	\$57	\$195
	800	8.00	\$156	\$107	\$263
	1600	10.00	\$195	\$214	\$409
	3525	14.81	\$289	\$472	\$761
Car	Cost per mile: \$0.260	Avg. Speed: 60			
	Trip Length	Time (hours)	Time Cost	Travel Cost	Total Cost
	250	4.17	\$81	\$65	\$146
	425	7.08	\$138	\$111	\$249
	800	13.33	\$260	\$208	\$468
	1600	42.67	\$832	\$416	\$1248
	3525	114.75	\$2238	\$917	\$3154
Amtrak	Cost per mile: \$0.257	Avg. Speed: 45			
	Trip Length	Time (hours)	Time Cost	Travel Cost	Total Cost
	250	5.56	\$108	\$64	\$173
	425	9.44	\$184	\$109	\$293
	800	17.78	\$347	\$206	\$552
	1600	35.56	\$693	\$411	\$1105
	3525	78.33	\$1528	\$906	\$2433
Best Alternative	Trip Length	Total Cost	Total Cost	Total Cost	
		Change	Change Pct.	Change/Mile	
Car	250	-\$16	-10%	\$0.066	
Car	425	\$54	28%	\$0.127	
Car	800	\$205	78%	\$0.256	
Amtrak	1600	\$695	170%	\$0.434	
Amtrak	3525	\$1672	220%	\$0.474	

With an elasticity of -1 , for example, for every 10 percent increase in the price of travel, 10 percent fewer people will be willing to pay to make the trip. Put the other way, 90 percent of people would value air travel enough to pay 10 percent more to still make the trip.

To estimate the change in consumer surplus when air travel is disrupted, we first calculate how many people paid what price when they were able to fly, and then we calculate how many people would be willing to pay the price of taking the best alternative mode of travel. We compare how much higher the price of the alternative is and how many people decided to cancel their trip. Those that cancel have lower values of making the trip and lose the consumer surplus they would have received from their travel. Those that still travel by the alternative lose consumer surplus from the higher price they have to pay.³

³ In estimating the number of travelers who would still take the trip using an alternative mode, we assume that tastes for travel and income levels do not change, neither of which may hold true in the event of a catastrophic terrorist attack. An attack could also affect the preference between car and train for travel in the aftermath. However, the nature and size of the effect is uncertain *a priori* and is not included here.

Table A.2
(continued)

Business Travel					
Airline	Time cost: \$34.50	Cost per mile: \$0.134	Avg. Speed: 400		
	Trip Length	Time (hours)	Time Cost	Travel Cost	Total Cost
	250	6.63	\$229	\$34	\$262
	425	7.06	\$244	\$57	\$301
	800	8.00	\$276	\$107	\$383
	1600	10.00	\$345	\$214	\$559
	3525	14.81	\$511	\$472	\$983
Car	Cost per mile: \$0.260		Avg. Speed: 60		
	Trip Length	Time (hours)	Time Cost	Travel Cost	Total Cost
	250	4.17	\$144	\$65	\$209
	425	7.08	\$244	\$111	\$355
	800	13.33	\$460	\$208	\$668
	1600	42.67	\$1472	\$416	\$1888
	3525	114.75	\$3959	\$917	\$4875
Amtrak	Cost per mile: \$0.257		Avg. Speed: 45		
	Trip Length	Time (hours)	Time Cost	Travel Cost	Total Cost
	250	5.56	\$192	\$64	\$256
	425	9.44	\$326	\$109	\$435
	800	17.78	\$613	\$206	\$819
	1600	35.56	\$1227	\$411	\$1638
	3525	78.33	\$2703	\$906	\$3608
Best Alternative	Trip Length	Total Cost		Total Cost	Total Cost
		Change	Change Pct.	Change/Mile	
Car	250	-\$53	-20%	-\$0.213	
Car	425	\$54	18%	\$0.356	
Car	800	\$285	74%	\$0.128	
Amtrak	1600	\$1078	193%	\$0.674	
Amtrak	3525	\$2625	267%	\$0.745	

SOURCES: Runzheimer International, Amtrak, Air Transport Association

In Table A.3, to calculate the consumer welfare, the trip-distance mileage-share calculations from Table A.1 are first applied to revenue passenger mile data. This generates the number of miles traveled for each trip distance and purpose category. Price elasticities of demand for business and leisure travelers are used to translate the cost changes for the best travel alternative from Table A.2 into welfare changes. Welfare changes are then calculated for a systemwide shutdown of a day, a week, and a month.

As mentioned previously, most international air travel does not have a realistic alternative. Accordingly, we assume a price increase for air travel large enough to preclude essentially all demand. Welfare changes are also calculated for international travel. Using this approach, combined consumer welfare losses from a month-long shutdown of domestic and international flights would top \$8 billion, while a week's shutdown would incur about \$2 billion worth of lost travel value.

Table A.3
Consumer Surplus Loss (Domestic)
 (all miles and dollars in billions, except cost change in dollars per mile)

Domestic								
Revenue Passenger Miles (2001): 480 Business/Leisure split: 50%					Shutdown Cost of			
Business Miles: 240 Price Elasticity of Demand: -0.7					One Month			
RT Mileage					One Month			
RT Mileage	Percentage of Total Miles	Miles	Total Cost Change per Mile	Travel Cost Change Pct.	One Day	One Week		
<300	0.1%	0.3	-\$0.213	-20%	\$0.00	\$0.00		
300-499	1.1%	2.7	\$0.128	18%	\$0.00	\$0.01		
500-999	7.9%	19.0	\$0.356	74%	\$0.01	\$0.10		
1,000-1,999	21.4%	51.4	\$0.674	193%	\$0.04	\$0.25		
>2,000	69.4%	166.4	\$0.745	267%	\$0.09	\$0.64		
Domestic business subtotal					\$0.14	\$0.98		
					\$4.21			
Leisure miles: 240 Price elasticity of demand: -1.0								
Shutdown Cost of								
RT Mileage					One Month			
RT Mileage	Percentage of Total Miles	Miles	Total Cost Change per Mile	Travel Cost Change Pct.	One Day	One Week		
<300	0.1%	0.3	-\$0.066	-10%	\$0.00	\$0.00		
300-499	1.1%	2.7	\$0.127	28%	\$0.00	\$0.01		
500-999	7.9%	19.0	\$0.256	78%	\$0.01	\$0.06		
1,000-1,999	21.4%	51.4	\$0.434	170%	\$0.02	\$0.13		
>2,000	69.4%	166.4	\$0.474	220%	\$0.05	\$0.34		
Domestic leisure subtotal					\$0.08	\$0.53		
					\$2.28			
Domestic subtotal					\$0.22	\$1.52		
					\$6.50			
International								
Revenue Passenger Miles (2001): 175.8 Business/Leisure split: 50%					Shutdown Cost of			
Business Price Elasticity: -0.7 Leisure Price Elasticity: -1.0					One Month			
RT Mileage					One Month			
RT Mileage	Miles	Total Cost Change per Mile	Travel Cost Change Pct.	One Day	One Week	One Month		
Business miles					\$0.04	\$0.29		
Leisure miles					\$0.02	\$0.15		
International subtotal					\$0.06	\$0.44		
					\$1.92			
Domestic and international subtotal					\$0.28	\$1.96		
					\$8.42			

SOURCE: Air Transport Association

Table A.4
Producer Surplus Loss
 (all miles and dollars in billions, except revenue per passenger mile in dollars per mile)

	System Shutdown of		
	One Day	One Week	One Month
Domestic			
Revenue Passenger Miles (2001)	1.31	9.20	39.41
Revenue per Passenger Mile (2001)	\$0.134	\$0.134	\$0.134
Domestic Airline Revenue	\$0.2	\$1.2	\$5.3
International			
Revenue Passenger Miles (2001)	0.48	3.37	14.45
Revenue per Passenger Mile (2001)	\$0.097	\$0.097	\$0.097
International Airline Revenue	\$0.0	\$0.3	\$1.4
Subtotal	\$0.22	\$1.56	\$6.68
Percent of costs incurred	87%	87%	84%
Total	\$0.19	\$1.36	\$5.61

SOURCE: Air Transport Association

For consistency, Table A.4 shows producer surpluses in a similar format. Combining the numbers from Tables A.3 and A.4, the sum of consumer and producer surpluses tops \$3 billion for a one-week shutdown and comes to \$14 billion for one month.

APPENDIX B

Congressional Bills

Listed are two relevant congressional bills introduced during 2003 and 2004 dealing with countermeasures installation aboard commercial airliners.

HR 4056 IH 108th CONGRESS 2d Session, H. R. 4056

To encourage the establishment of both long-term and short-term programs to address the threat of man-portable air defense systems (MANPADS) to commercial aviation.

IN THE HOUSE OF REPRESENTATIVES

March 30, 2004

Mr. MICA (for himself, Mr. DEFAZIO, and Mr. ISRAEL) introduced the following bill; which was referred to the Committee on Transportation and Infrastructure, and in addition to the Committee on International Relations, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

A bill:

To encourage the establishment of both long-term and short-term programs to address the threat of man-portable air defense systems (MANPADS) to commercial aviation.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the 'Commercial Aviation MANPADS Defense Act of 2004'.

SEC. 2. FINDINGS.

Congress finds the following:

- (1) MANPADS constitute a threat to military and civilian aircraft.
- (2) The threat posed by MANPADS requires the development of both short-term and long-term plans.
- (3) The threat posed by MANPADS requires an international as well as domestic response.
- (4) There should be an international effort to address the issues of MANPADS proliferation and defense.
- (5) The Government is pursuing and should continue to pursue diplomatic efforts to prevent the proliferation of MANPADS.

SEC. 3. INTERNATIONAL COOPERATIVE EFFORTS.

- (a) To Limit Availability and Transfer of MANPADS- The President is encouraged to pursue further strong international diplomatic and cooperative efforts, including bilateral and multilateral

treaties, in the appropriate forum to limit the availability, transfer, and proliferation of MANPADS worldwide.

(b) To Achieve Destruction of MANPADS- The President should continue to pursue further strong international diplomatic and cooperative efforts, including bilateral and multilateral treaties, in the appropriate forum to assure the destruction of excess, obsolete, and illicit stocks of MANPADS worldwide.

(c) Reporting and Briefing Requirements- Not later than 180 days after the date of enactment of this Act, the President shall transmit to the appropriate congressional committees a report that contains a detailed description of the status of diplomatic efforts under subsections (a) and (b). Annually thereafter until completion of such diplomatic efforts, the Secretary of State shall brief the appropriate congressional committees on the status of such diplomatic efforts.

SEC. 4. FAA AIRWORTHINESS CERTIFICATION OF MISSILE DEFENSE SYSTEMS FOR COMMERCIAL AIRCRAFT.

(a) In General- Not later than 30 days after the date of enactment of this Act, the Administrator of the Federal Aviation Administration shall establish a process for conducting airworthiness and safety certification of missile defense systems for commercial aircraft.

(b) Certification Acceptance- Under the process, the Administrator shall accept the certification of the Department of Homeland Security that a missile defense system is effective and does not pose a danger when used to defend commercial aircraft against MANPADS.

(c) Expedited Certification- Under the process, the Administrator shall expedite the airworthiness and safety certification of missile defense systems for commercial aircraft.

(d) Reports- Not later than 180 days after the initiation of certification procedures for missile defense systems for commercial aircraft, and every 6 months thereafter until complete, the Federal Aviation Administration shall transmit to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report that contains a detailed description of the status of airworthiness and safety certification.

SEC. 5. PROGRAMS TO REDUCE MANPADS.

(a) In General- The President is encouraged to pursue strong programs to reduce the number of MANPADS worldwide so that fewer MANPADS will be available for trade, proliferation, and sale.

(b) Reporting and Briefing Requirements- Not later than 180 days after the date of enactment of this Act, the President shall transmit to the appropriate congressional committees a report that contains a detailed description of the status of the programs being pursued under subsection (a). Annually thereafter until the programs are no longer needed, the Secretary of State shall brief the appropriate congressional committees on the status of programs.

(c) Funding- There is authorized to be appropriated such sums as may be necessary to carry out this section.

SEC. 6. MANPADS VULNERABILITY ASSESSMENTS REPORT.

(a) In General- Not later than one year after the date of enactment of this Act, the Secretary of Homeland Security shall transmit to the Committee on Transportation and Infrastructure of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report describing the Department of Homeland Security's plans to secure airports and the aircraft arriving and departing from airports against MANPADS attacks.

(b) Matters to Be Addressed- The Secretary's report shall address, at a minimum, the following:

(1) The status of the Department's efforts to conduct MANPADS vulnerability assessments at United States airports at which the Department is conducting assessments.

(2) How intelligence is shared between the United States intelligence agencies and Federal, State, and local law enforcement to address the MANPADS threat and potential ways to improve such intelligence sharing.

(3) Contingency plans that the Department has developed in the event that it receives intelligence indicating a high threat of MANPADS attack on aircraft at or near United States airports.

(4) The feasibility and effectiveness of implementing public education and neighborhood watch programs in areas surrounding United States airports in cases in which intelligence reports indicate there is a high risk of MANPADS attacks on aircraft.

(5) Any other issues that the Secretary deems relevant.

(c) Format- The report required by this section may be submitted in a classified format.

SEC. 7. DEFINITIONS.

In this Act, the following definitions apply:

(1) Appropriate congressional committees- The term 'appropriate congressional committees' means—

(A) The Committee on Armed Services, the Committee on International Relations, and the Committee on Transportation and Infrastructure of the House of Representatives; and

(B) the Committee on Armed Services, the Committee on Foreign Relations, and the Committee on Commerce, Science, and Transportation of the Senate.

(2) MANPADS- The term 'MANPADS' means man-portable air defense systems, which are shoulder-fired, surface-to-air missile systems that can be carried and transported by a person.

HR 580 IH 108th CONGRESS 1st Session, H.R. 580

To direct the Secretary of Transportation to issue regulations requiring turbojet aircraft of air carriers to be equipped with missile defense systems, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

February 5, 2003

Mr. ISRAEL introduced the following bill; which was referred to the Committee on Transportation and Infrastructure, and in addition to the Committee on Armed Services, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

A bill:

To direct the Secretary of Transportation to issue regulations requiring turbojet aircraft of air carriers to be equipped with missile defense systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the 'Commercial Airline Missile Defense Act'.

SEC. 2. REGULATIONS REQUIRING MISSILE DEFENSE SYSTEMS.

(a) IN GENERAL- Not later than 90 days after the date of enactment of this Act, the Secretary of Transportation shall issue regulations that require all turbojet aircraft used by an air carrier for scheduled air service to be equipped with a missile defense system.

(b) SCHEDULE FOR INSTALLATION- The regulations shall establish a schedule for the purchase and installation of such systems on turbojet aircraft currently in service and turbojet aircraft contracted for before the date of issuance of the regulations.

(c) NEW AIRCRAFT- The regulations shall also require that all turbojet aircraft contracted for on or after the date of issuance of the regulations by an air carrier for scheduled air service be equipped with a missile defense system.

(d) DEADLINES FOR COMMENCEMENT OF INSTALLATION- The regulations shall require that installation and operation of missile defense systems under the regulations begin no later than December 31, 2003.

SEC. 3. PURCHASE OF MISSILE DEFENSE SYSTEMS BY THE SECRETARY.

The Secretary of Transportation shall purchase and make available to an air carrier such missile defense systems as may be necessary for the air carrier to comply with the regulations issued under section 2 (other than subsection (c)) with respect to turbojet aircraft used by the air carrier for scheduled air service.

SEC. 4. RESPONSIBILITY OF AIR CARRIER.

Under the regulations issued under section 2, an air carrier shall be responsible for installing and operating a missile defense system purchased and made available by the Secretary of Transportation under section 3.

SEC. 5. PROGRESS REPORTS.

Not later than January 1, 2004, and each July 1 and January 1 thereafter, the Secretary of Transportation shall transmit to Congress a report on the progress being made in implementation of this Act, including the regulations issued to carry out this Act.

SEC. 6. INTERIM SECURITY MEASURES

(a) IN GENERAL- In order to provide interim security before the deployment of missile defense systems for turbojet aircraft required under section 2, the President shall—

(1) exercise the President's authority under title 32, United States Code, to elevate National Guard units to Federal status for the purpose of patrolling airport areas surrounding airports against the threat posed by missiles and other ordinance to commercial aircraft; and

(2) deploy units of the United States Coast Guard, in coordination with the Secretary of Transportation and the Secretary of Homeland Security, for the purpose of patrolling areas surrounding airports to protect against the threat posed by missiles and other ordinance to commercial aircraft.

(b) PROGRESS REPORT- Not later than 90 days after the date of enactment of this Act, the President shall submit to Congress a report on the progress being made to implement this section.

SEC. 7. DEFINITIONS.

In this Act, the following definitions apply:

(1) AIRCRAFT AND AIR CARRIER- The terms 'aircraft' and 'air carrier' have the meaning such terms have under section 40102 of title 49, United States Code.

(2) MISSILE DEFENSE SYSTEM- The term 'missile defense system' means an appropriate (as certified by the Secretary of Transportation) electronic system that would automatically—

(A) identify when the aircraft is threatened by an incoming missile or other ordinance;

(B) detect the source of the threat; and

(C) disrupt the guidance system of the incoming missile or other ordinance, which is intended to result in the incoming missile or other ordinance being diverted off course and missing the aircraft.

References

Air Transport Association, Economics Home Page, June 21, 2003, <http://www.airlines.org/econ/p.aspx?nid=6342> (as of November 3, 2003).

_____, Airline Industry Facts, Figures, and Analyses, <http://www.airlines.org/econ/d.aspx?nid=1026> (as of November 3, 2003).

Benjamin, D., and S. Simon, *The Age of Sacred Terror*, New York: Random House, 2002.

Bolkcom, C., B. Elias, and A. Feickert, *Congressional Research Service Report for Congress: Homeland Security: Protecting Airliners from Terrorist Missiles*, Washington, D.C.: Congressional Research Service 2003.

Caffera, P., "U.S. Jets Easy Target for Shoulder-Fired Missiles," *San Francisco Chronicle*, November 30, 2002, p. A14.

CNN, "Feds Tell How the Weapons Sting Was Played," CNN.com, August 14, 2003, <http://cnn.com/2003/LAW/08/13/arms.sting.details/> (as of November 3, 2003).

CSIS, "Transnational Threats Update," Vol. 1, No. 10, 2003, p.2.

Cullen, Tony, and Christopher F. Foss, eds., *Jane's Air Defense Systems, 2001–2002*, Surrey, England: Jane's Information Group, 2001.

Department of Defense, "FY 2004/2005 President's Budget Item Justification," R-2 RDT&E Exhibit, February 2003.

Department of Homeland Security, "FY2004 Budget Fact Sheet," October 15, 2004, <http://www.dhs.gov/dhspublic/display?content=1817> (as of October 2003).

Department of Justice, September 11th Victim Compensation Fund of 2001: Compensation for Deceased Victims, http://www.usdoj.gov/victimcompensation/payments_deceased.html (as of July 19, 2004).

Dixon, L., *Assistance and Compensation for Individuals and Businesses after the September 11th Terrorist Attacks*, Santa Monica, Calif.: RAND Corporation, MG-264-ICJ, forthcoming.

Erwin, S., "Anti-Missile Program for Airliners on a Fast Track," *National Defense*, December 2003, <http://www.nationaldefensemagazine.org/article.cfm?Id=1281> (as of February 1, 2004).

Federal Aviation Administration, "Economic Values for Evaluation of FAA Investment and Regulatory Programs," U.S. Department of Transportation, FAA-APO-98-8, June 1998.

Department of the Air Force, *Fiscal Year (FY) 2004/2005 Biennial Budget Estimates, Research, Development, Test and Evaluation (RDT&E), Descriptive Summaries*, Vol. III, Budget Activity 7, February 2003, pp. 1837–1843.

Gusinov, T., "Portable Missiles May Become Next Weapon of Choice for Terrorists," *Washington Diplomat*, June 16, 2003, www.washingtondiplomat.com/03_01/a4_03_01.html (as of March 4, 2004).

Jane's Terrorism and Insurgency Centre, "Proliferation of MANPADS and the Threat to Civil Aviation," August 13, 2003, http://www.janes.com/security/international_security/news/jtic/jtic030813_1_n.shtml (as of September 17, 2003).

Kuhn, D., "Mombassa Attack Highlights Increasing MANPADS Threat," *Jane's Intelligence Review*, February 2003, pp. 26-31.

Morrison, Steven A., and Clifford Winston, "An Econometric Analysis of the Demand for Intercity Passenger Transportation," *Research in Transportation Economics*, Vol. 2, 1985, pp. 213-37.

Office of Management and Budget, "FY-2004 Supplemental Appropriations Request," Washington, D.C., September 17, 2003.

Pedriani, C., "JASPO/NASA Cooperate to Improve Commercial Aviation Security," in *Aircraft Survivability: Reclaiming the Low Altitude Battlespace*, Joint Aircraft Survivability Program Office, 2003.

Popp, M., "Cost Analysis Update," briefing to the Interagency Task Force, NAVAIR 4.2V, February 13, 2003.

Townsend, J., "15 SOS Field Support Visit Aircraft Modernization" unclassified briefing, HQ AFSOC/XPQA, Hurlburt AFB, January 23, 2001.

Turner, B., "Aviation Demand Forecasts, Large Air Carriers-Passengers, Fiscal Years 2003-2014," FAA, February 13, 2003.

Victoria Transport Policy Institute, "Transportation Costs and Benefits," www.vtpi.org/tdm/tdmbb.htm (as of July 13, 2004).

Wilbur Smith Associates, "The Economic Impact of Civil Aviation on the U.S. Economy," April 2003.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Susan Collins

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 1.

Given the wide range of activities over which the Department of Homeland Security has influence, it is essential that DHS coordinate its activities with other federal agencies. For example, bioterrorism responsibilities are divided between HHS and DHS. Do you think this division has worked to date, and if not, how do you think these responsibilities should be reallocated?

Answer.

We have not reviewed the topic of segregation of duties related to preventing and responding to incidents of biological terrorism. However, we recently initiated an audit of DHS's BioWatch program. The overall objective of our audit is to determine to what extent DHS has designed and implemented management controls to coordinate the BioWatch program among the partner agencies and accomplish its objectives. The partner agencies include the Environmental Protection Agency (EPA) and the Centers for Disease Control and Prevention (CDC), a Department of Health and Human Services (HHS) agency. The EPA provides services and technical expertise to the program that includes establishing, deploying, operating, and maintaining network sensors. The CDC provides, among other things, technical expertise and laboratory analysis services. We are coordinating our review with the Department of Health and Human Services Office of Inspector General and the Environmental Protection Agency Office of Inspector General.

Question 2.

Are there adequate plans for the medical response to a bioterrorism attack, and are these plans the product of adequate coordination between DHS and HHS?

Answer.

We have not reviewed these plans and have no basis on which to address the question at this time.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Susan Collins

"The Department of Homeland Security: The Road Ahead"

January 26, 2005

Question 3.

During the 1990s, the Justice Department developed two different, incompatible fingerprint screening programs – IDENT was developed by the INS, and IAFIS was developed by the FBI. It has been a challenge for years to integrate these programs, a challenge made more difficult by moving the IDENT program over to DHS. The integration of these systems is critically important, especially given the fact that US-VISIT uses the IDENT system. Are these systems compatible, and if not, what will it take to make them compatible?

Answer.

We have not examined the integration of the Department of Homeland Security's (DHS) Automated Biometric Identification System (IDENT) and the Department of Justice's (DOJ) Integrated Automated Fingerprint Identification System (IAFIS) fingerprint systems. However, there is a wealth of information on this subject that is the result of four DOJ Office of Inspector General (OIG) reports issued over the last four years with the most recent being issued December 2004. While considerable progress has been made to integrate the two fingerprint systems, full integration still appears to be some years away.

The latest DOJ OIG report highlighted several areas of concern regarding the integration project. DHS and the Department of State (DOS) have not agreed to implement the January 2003 Technology Standard, developed by the National Institute of Standards and Technology (NIST), jointly with the Attorney General and the Secretary of State, at the direction of Congress, as the uniform method for collecting fingerprint information and for searching against large databases. NIST research showed that taking ten flat fingerprints, versus taking ten "rolled" fingerprints, offered a technologically and operationally acceptable approach for DOJ, DHS, and DOS to screen incoming travelers.

Accordingly, the NIST Technology Standard is for ten flat fingerprints to be taken to add or "enroll" individuals in databases and to conduct searches of the databases. NIST further recommended that two flat fingerprints and a digital picture be used to verify the identity of a person against an existing record, but not for enrollment. DHS' United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program uses the two flat fingerprint IDENT system to enroll foreign travelers entering the United States. This procedure is not consistent with the NIST-recommended Technology Standard.

DHS and DOJ disagree on providing access to IDENT database information to federal, state, and local law enforcement agencies as specified in the U.S. PATRIOT Act and in subsequent congressional legislation. DHS does not believe that the Federal Bureau of Investigation or other law enforcement agencies should have access to US-VISIT records. DHS maintains this position because of concerns that the information in IDENT is incomplete and could be misinterpreted, and to protect the privacy of travelers enrolled in US-VISIT. Without direct access to DHS' IDENT database, it is more difficult for federal, state, and local law enforcement agencies to identify illegal aliens that they encounter.

Finally, because IDENT and IAFIS integration has not been achieved, DHS continues to rely on records manually extracted from IAFIS and entered into IDENT for most fingerprint searches. The extracted data represents only a small portion of the more than 47 million records in the IAFIS Criminal Master File. The fingerprint file of "Known or Suspected Terrorists" is only transmitted to DHS once a month. Consequently, criminals or terrorists could be missed by checks against the extracted records.

According to a DOJ study published in August 2004, almost three quarters (73.1 %) of the criminal aliens encountered at Border Patrol stations and ports of entry were identified only by checking IAFIS, and would not have been identified by checking IDENT. The results clearly showed that not checking aliens against IAFIS increases the risk that we will unknowingly admit criminal aliens.

While US-VISIT has been successful in interdicting some known criminals attempting to enter the United States, the DOJ study is disturbing because it seems to indicate that not all known criminals can be identified through the use of IDENT alone. US-VISIT officials estimate that only 0.7 % of all foreign travelers will have their fingerprints queried in IAFIS. The vast majority, 99.3 % will be screened using IDENT only. US-VISIT, which uses IDENT, itself processes few foreign travelers. At land POEs, for example, only 2.7% of foreign travelers are processed through US-VISIT/IDENT. DOJ proposed conducting a similar study using data from visitors enrolled in US-VISIT, but DHS has not yet agreed to do so. However, we are now exploring the possibility of conducting such a study.

Question 4.

Can you comment on DHS's progress with the development and deployment of biometric identification systems in general and TWIC in particular? How do you view the priority they have given this program, more than three years after 9/11?

Answer.

DHS' highest-profile biometric system undoubtedly has been US-VISIT. The rollout of this system has been smooth and uneventful. The arrival module is in place at all international airports and now at the busiest land crossings; it continues to be expanded to the facilities not yet connected. The departure module is being piloted at present. With specific reference to TSA's Transportation Worker Identification Credential (TWIC) program, our office has not yet examined this program and is not aware of any problems TSA might be encountering.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Susan Collins

"The Department of Homeland Security: The Road Ahead"

January 26, 2005

Question 5.

Can you discuss how DHS should ensure the interoperability and compatibility of the various biometric identification systems that have been deployed and are being developed by DHS and other agencies?

Answer.

We have not conducted work in this area, however, it is clear that DHS, like many other agencies, should employ better standardization between its various biometric identification systems, independent of the underlying identification technology, i.e., fingerprint scanning, retina scanning, etc. For example, if DHS were to adopt a common data format and method of exchange, it may be possible to have a retina scanner and a fingerprint scanner "speak" to the same core system -- and share information.

Currently - some standards do exist. For example, *NIST Special Publication 800-76 "Biometric Data Specification for Personal Identity Verification"* (<http://csrc.nist.gov/publications/drafts.html#sp800-76>) addresses various specification requirements and options for fingerprints and facial images. However, it lacks specifications and guidelines for many other common types of biometric identification, such as retina scans, thermal scans, etc.

Also, NIST published *NISTIR 6529, "Common Biometric Exchange File Format"* (CBEFF; <http://www.nist.gov/cbeff>). This underlying data format, when used in conjunction with a standardized method of access, such as the BioAPI Specification (<http://www.bioapi.org/BIOAPI1.1.pdf>), is essential to the development and implementation of biometric identification systems that are compatible and interoperable.

Although the CBEFF is a NIST standard, the BioAPI Specification is a standard based on an industry consortium comprised of biometric vendors. This consortium is akin to the W3C, the consortium that develops interoperable technologies and standards for the World Wide Web, such as HTML guidelines. DHS needs to assess these standards and determine which one will best meet its needs, as well as the needs of agencies with which it must interoperate.

Unfortunately, creating or adopting existing standards may not help the legacy systems that are already in place. If these systems are not compliant with DHS-adopted standards, they may not be able to communicate with other biometric identification systems. There are several possible solutions to this:

- 1) Replace current systems with one that adheres to standards;
- 2) Re-engineer systems to adhere to standards, and
- 3) Create an intermediary process that captures, duplicates, and standardizes data for inter-system use.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Susan Collins

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 6.

In general, have DHS activities in the areas of technology development, preparedness, and intelligence been adequately coordinated with other federal agencies? If not, what recommendations would you make to improve this coordination?

Answer.

We have not reviewed DHS' coordination of technology development, preparedness, and intelligence with other federal agencies, and have no basis on which to address the question at this time.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Daniel Akaka

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 1.

The 27 Visa Waiver Program (VWP) countries have been given until October 26, 2005, to incorporate a facial biometric identifier into their passports. Most VWP countries are struggling to meet that goal because the process costs millions of dollars.

Secretary Ridge recently made a number of public statements arguing that the United States should incorporate biometric data into U.S. passports before we can ask the rest of the world to do so. However, no specific timeline was given.

You stated that you believe the Department of Homeland Security (DHS) needs to decide on a biometric identifier soon and incorporate it into U.S. travel documents.

What feedback, if any, did you receive from the Department on this recommendation and did they provide you a date for this decision?

Answer.

As you note, the Secretary has already publicly raised the issue of fingerprints in U.S. passports. Including them would enhance the security of the document. Our current practice – using a photograph mailed to us by the passport applicant – has obvious security weaknesses since we cannot easily verify that the photograph is of the person whose biographic particulars are written on the passport application form.

The first biometric passports are about to appear. The international effort has been coordinated by the standards-setting organization for international air travel, the United Nations International Civil Aviation Organization (ICAO). ICAO needed to move quickly despite a lack of international consensus on the cultural implications of fingerprinting. It therefore required only a photograph be digitally encoded in the first generation of passports, but made room in the standard for nations to include fingerprints in their passports if they chose to do so. The United States Government has not yet decided to do so. We do not have any information as to whether or when these questions might be considered.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Daniel Akaka

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 2.

On September 22, 2004, the Transportation Security Administration (TSA) updated its secondary screening policy to include pat-down searches for randomly selected passengers who had not triggered any other alarm in the system. This was intended to heighten TSA's ability to detect explosives hidden on a person.

However, TSA modified its policy to exclude a pat-down of the torso region without any explanation.

You stated that your office is currently reviewing the implementation of the current procedures. Has your office conducted any investigations into the decision-making process that led up to the heightened screening procedures and the subsequent modification? If so, will you comment on the foundation for these policy changes?

Answer.

We have not conducted an investigation into the decision-making process that led up to the heightened screening procedures and the subsequent modifications. However, at the request of Congress, our office is conducting an audit of TSA's updated secondary screening procedures. Our audit objectives are to determine whether TSA adequately advises passengers of their rights under the screening process, and how well TSA accommodates requests related to those rights; whether secondary screening practices are applied proportionately to males and females; whether screeners are adequately trained to perform pat-down searches; and whether TSA has procedures for investigating and resolving complaints about the secondary screening process.

On December 23, 2004, TSA issued new guidelines that modified its updated secondary screening policies. The modified procedures called for patting down the chest area only if the passenger alarmed a hand-held metal detector or if the screener detected an irregularity or anomaly in the person's clothing outline. Unless these criteria are met, screeners will only pat-down a line below the chest area to the waist, followed by a pat-down of the individual's back. TSA officials said they modified the procedures as a result of new intelligence information.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Daniel Akaka

"The Department of Homeland Security: The Road Ahead"

January 26, 2005

Question 3.

In a September 2004 report, your office found that TSA mismanaged a contract with Boeing to install Explosive Detection Systems and overpaid Boeing by approximately \$49 million.

In your December 2004 report, which is one of the subjects of today's hearing, you state that while TSA lacked adequate contract oversight in the past, policies and procedures are being implemented to provide better planning, structure, and oversight of contracts.

Will you please describe what policies TSA is putting in place, and would you comment on what more needs to be done to strengthen the transparency and accountability of TSA's contracts?

Answer.

TSA has developed and implemented several program management and acquisition policies since the airport federalization process in December 2002 for strengthening project management and contract planning and oversight throughout the acquisition lifecycle. In conjunction with DHS requirements, TSA has begun implementing certification requirements for program managers and contracting professionals. All program managers and contracting professionals must have a certification commensurate to the size and complexity of the assigned acquisition program. The certification processes consider the level of education, training, and work experience of program managers and contracting professionals to determine the eligibility for certification and the appropriate certification level.

TSA has also established an Acquisition and Program Management Support Division (PM Support Division) that provides program management support and develops acquisition policy relating to the acquisition life cycle process. To date, the PM Support Division has developed and implemented a policy and guidance requiring acquisition plans for contracting actions exceeding \$5 million and a management directive that requires program offices to develop mission needs statements. The PM Support Division also intends to develop policies and guidance concerning other critical acquisition planning documents, such as life cycle cost estimates, cost-benefit analysis, operational requirements, and alternative analysis. The DHS Investment Review Board, which reviews and approves all TSA acquisitions exceeding \$50 million, requires many of these critical planning documents at key decision points in the acquisition life cycle process. Our report on the Boeing contract recommended that TSA develop policy and guidance on reasonable award fees for contracts. We believe that establishing and following accepted best practices in program management and acquisition will help TSA to improve their contracting procedures and obtain better results with greater accountability.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Daniel Akaka

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 4.

Both the Center for Strategic and International Studies-Heritage Foundation report, “DHS 2.0,” and the December 2004 DHS Inspector General (IG) report, “Major Management Challenges Facing the Department of Homeland Security,” state that the Chief Information Officer (CIO) lacks the necessary department-wide authority to administer the Department’s information technology policy.

To address my concerns about the lack of authority and resources in the CIO office to coordinate the Department’s geospatial policy, Congress gave additional authorities to the CIO and created an Office for Geospatial Management.

What further actions would you recommend, either through legislation or administrative action, to strengthen the CIO? Does the CIO need more authorities, more resources, or both?

Answer.

The issues that we raised in our Management Challenges report concern the authorities and resources of the central, department-wide CIO—not any individual component-level CIO. They also do not relate to any particular function or area, such as geospatial policy. We summarized these CIO issues based on our prior, July 2004 report, *“Improvements Needed to DHS’ Information Technology Management Structure.”*

In July 2004 report, we emphasized that the CIO needs both greater authority and resources to carry out required strategic IT management responsibilities. For example, we said that by reporting to the Under Secretary for Management several layers down within the department, the CIO has no authority over the more senior component directors that he is supposed to be advising and overseeing in terms of IT. Without a documented, formal relationship whereby the CIOs of the major DHS component organizations report to him, the DHS CIO does not have the power or influence to guide IT initiatives across the department to help accomplish his goals of creating within DHS “one network, one infrastructure.” Further, given his small staff of 65 versus the much larger IT organizations of the component organizations, the DHS CIO has inadequate support to meet the many challenges in providing IT services and consolidating technology systems, facilities, and initiatives across 22 different components in the new department. We said that the deficiencies in the CIO’s positioning and authority are exemplified by the limited role he plays in the department’s investment review process,

largely confined to consensus building to manage the infrastructure and selected joint or consolidated systems while mission applications and component level IT investments continue to be managed in a decentralized manner.

As such, we recommended repositioning the DHS CIO to report directly to the Office of the Deputy Secretary, thereby providing the CIO with the authority and the ability to influence senior executive decisions concerning department-wide IT investments and strategies. We urged the department to document and communicate the roles of component level CIOs, including their dual reporting relationships to the DHS CIO and heads of their respective DHS organizations, in order to ensure their support for and alignment with central policies, standards, and strategies for consolidating and integrating the department's IT infrastructure as well as mission and business objectives. We recommended providing the DHS CIO office with the staff resources necessary to facilitate accomplishment of department-wide IT consolidation objectives and supporting initiatives. Further, we advised assigning the CIO a key role in all levels of the department's investment review process to ensure, guide, and document timely and effective IT investment decisions to support accomplishment of department-wide business objectives.

In responding to our recommendations, the Deputy Secretary did not concur with repositioning the CIO to report directly to the Office of the Deputy Secretary. The Deputy Secretary said that the current arrangement in which the CIO reports directly to the Under Secretary for Management does not hinder or preclude the CIO from performing all essential job-related requirements. The Deputy Secretary said that the priorities of the Secretary, Deputy Secretary, and DHS are known throughout the chain of command and the responsible individuals have the inherent authority to accomplish these tasks. We do not agree with the Deputy Secretary's response and believe that corrective action is still needed to meet Federal requirements and position the CIO as a member of the senior executive team with the accountability and responsibility to manage IT across organizational units.

The Deputy Secretary nonetheless has outlined plans to establish formal reporting relationships between the DHS CIO and the CIOs of the major component organizations. The Deputy Secretary said that all departmental component CIOs will support the DHS CIO in all IT matters without exception, in addition to reporting to their respective agency heads. The formalized relationships and descriptions of duties are to be published in the department's organization manual, with interim guidance provided as needed. The Deputy Secretary said that the department is constantly striving to provide optimal resources through all DHS components and will look for further opportunities to re-program critical resources and personnel during the process of centralizing IT support services. Additionally, while the Deputy Secretary asserted that the CIO is already an integral member at all levels of the IT investment review process, he recommended adding the CIO as a member of the Level 2 Joint Requirements Council responsible for non-IT issues, thereby providing an element of crosscutting and situational awareness. We are awaiting updated information from the Deputy Secretary on the status of these proposed actions in order to evaluate the extent to which they satisfy concerns that we raised in our report.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Daniel Akaka

"The Department of Homeland Security: The Road Ahead"

January 26, 2005

Question 5.

The IG report notes the lack of language training for temporary duty officers serving overseas in the Border Security and Transportation Directorate.

Can you describe the overall language capabilities of the Department and provide your recommendations for increasing the number of personnel possessing critical language skills?

Answer.

The moment DHS was established, it inherited a considerable overseas presence. The former INS had employees assigned to embassies and consulates in 46 foreign cities in 34 countries. The former Customs Service had employees in 40 foreign cities in 30 countries. Other DHS components with international contingents included the Transportation Security Agency, with officers attached to 13 embassies and one consulate general; the U.S. Coast Guard, with personnel attached to 12 embassies; the U.S. Secret Service, represented at 18 U.S. embassies and consulates; and the Animal and Plant Health Inspection Service (APHIS), with personnel at approximately 30 posts abroad.

Overseas activities have expanded in the past 2 years. Many DHS employees are in the Middle East in support of various Iraq-related training activities. The Container Security Initiative (CSI) now has CBP and ICE employees in several dozen foreign ports. The ICE Visa Security Unit has employees in Saudi Arabia and expects to open new offices in other countries this year.

To the best of our knowledge, there has been only a very limited coordination of overseas activities. DHS has not yet completed a census of overseas personnel assets or made discernible effort to rationalize our foreign presence. Foreign operations remain fractured - conducted component by component without any synthesis. There is no interest yet in creating a foreign service of multi-functional generalist officers with extensive foreign language capabilities. Each DHS component defines its own foreign needs, recruits from within, sets its own standards for training such officers before they depart, and has its own personnel system for replacing them when their assignment is completed.

While many DHS employees speak some foreign language, it is impossible to assess the Department's "overall language capabilities" without surveying the employees; we are unaware of any existing employee language skill inventory. With the exception of the Border Patrol's Spanish language training, the Department does not have a foreign language program. With respect to the ICE Visa Security Unit, unlimited language training is available through the Department of State's Foreign Service Institute, to which DHS is entitled access according to the State - DHS Memorandum of Understanding signed in July 2003.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Daniel Akaka

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 6.

The Center for Strategic and International Studies-Heritage Foundation report, “DHS 2.0,” noted that unclassified but sensitive information designations are made on an ad hoc, office-by-office basis and that there is no usable definition for the term and, no common understanding of how to control this information.

What impact has this had on the ability of the IG to carry out your mission and report on matters of government waste, fraud, and abuse?

Answer.

The Inspector General Act of 1978, Pub. L. No. 95-452, as amended, authorizes the Inspector General access to all records, documents or other material available to DHS that relates to its programs and operations. 5 U.S.C. Appendix, § 6(a)(1). Congress provided the Secretary of DHS with authority to prohibit the Inspector General from completing any audit, inspection, or investigation if necessary to prevent disclosure of certain types of information, to preserve the national security, or to prevent a significant impairment to U.S. interests. Specific types of information subject to the Secretary’s authority concern intelligence, counterintelligence, or counterterrorism matters; ongoing criminal investigations or proceedings; undercover operations; the identity of confidential sources, including protected witnesses; and other matters the disclosure of which would constitute a serious threat to persons or property authorized protection under 18 U.S.C. § 3056, 3 U.S.C. § 202, or any provision of the Presidential Protection Assistance Act of 1976 or a serious threat to national security. 5 U.S.C. Appendix, § 8I. If the Secretary exercises the authority in section 8I, he must notify the Inspector General who in turn must notify the President of the Senate, the Speaker of the House, and appropriate committees. Secretary Ridge did not invoke this authority during his tenure at DHS.

In January 2005, DHS issued Management Directive 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information, containing definitions of For Official Use Only (FOUO), Sensitive Security Information (SSI), and Protected Critical Infrastructure Information (PCII). The definitions for SSI and PCII in the management directive are the statutory definitions of these terms. The definition of FOUO information in the directive is very similar to that of the definition of “sensitive information” contained in the Computer Security Act of 1987, Pub. L. No. 100-235. In addition to the definition, the directive identifies eleven separate categories of information as examples of information to be protected as FOUO within DHS. To date,

we have not been denied access to any type of sensitive but unclassified information in the course of our work.

We occasionally have encountered hesitancy on the part of other DHS officials in authorizing release of information contained in our reports. DHS OIG policy is to make publicly available as much of our written product as possible without jeopardizing privacy, national security, or proprietary or other such interests. Sometimes, our views on public disclosure have differed from those of other DHS officials. Our reviews will examine departmental programs and activities, and virtually all matters that we think are important enough to warrant examination bear some relationship to a security issue. For example, can we identify the airport that we examined because of possible serious deviations from baggage screening protocols in response to a Senator's request? Can we identify the port facility or other grantee that received federal funding to mitigate a security weakness? Can we report the number of FTEs and funding provided for the Information Analysis and Infrastructure Protection Directorate? Can we discuss the number of commercial airline flights that are NOT covered by the Federal Air Marshals? Can we discuss deficiencies in the training given to baggage screeners? In all these cases, we were able to report the information to Congress, but not the public. We make every effort to mutually resolve these differences. Most debates over disclosure of information have resulted from a genuine security concerns, not from a desire to avoid embarrassment. It is not the criticism of DHS programs or activities, but the factual recitals that are the subject of these debates. We will continue to work together with DHS components to reach agreement on disclosure issues.

Question 7.

One concern I have is that the sharing of sensitive but unclassified information increases the use of non-disclosure agreements.

Do you have any information regarding the number of non-disclosure agreements and the increase in their use since September 11, 2001?

Answer.

OIG has no information regarding the number of non-disclosure agreements in DHS. While DHS did issue a new requirement for non-disclosure agreement in December 2004, that requirement has since been rescinded.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Daniel Akaka

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 8.

Since the creation of DHS, employee morale has been of great concern. Employees are fearful of the new human resources system and the possible erosion of their rights. They are also concerned about their ability to do their jobs effectively due to the internal organization of the Department.

Knowing that employee morale affects recruitment and retention efforts as well as an agency's mission, what recommendations do you have for improving employee morale and the Department's relationship with employee organizations?

Answer.

We have not conducted any reviews or studies concerning DHS employee morale or for improving DHS' relationships with employee organizations. However, in response to a request made by the Chairman of the Senate Homeland Security and Governmental Affairs Committee at a hearing on January 26, 2005, we have initiated a review that will examine the merits of merging the bureaus of Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE). While our review will not focus on recruitment, retention, and employee morale issues, these issues are likely to surface during our review. We plan to issue our report in the summer of 2005.

Question 9.

According to a report I requested from the Government Accountability Office on government data mining activities that was issued last May, the Department of Homeland Security had 11 data mining systems either planned or in operation, not including CAPPS II or its successor Secure Flight, that use personal information. Four of those systems use information from the private sector and eight of them use information from other government agencies.

- a. In your opinion, what is the best way to ensure that the use of personal information in data mining systems is not running afoul of privacy rights and protections?
- b. How do we ensure the accuracy and quality of the mined data, and how do we prevent its misuse?

Answer:

- a. In your opinion, what is the best way to ensure that the use of personal information in data mining systems is not running afoul of privacy rights and protections?

We have not conducted a comprehensive study of the best practices for maintaining privacy rights and protections in data mining systems. We are, nevertheless, aware of a number of technical approaches available to system developers or managers that can help address concerns in these areas. One approach, called anonymization, allows users of data mining systems to share information with others without disclosing the identity of individuals or supplying information of non-suspects. Another approach is to build authorization requirements into government systems for viewing data to ensure that only those who need to see the data do. Also, system developers can build audit logs into the computing system to identify and track inappropriate access to information and misuses of information.

- b. How do we ensure the accuracy and quality of the mined data, and how do we prevent its misuse?

A number of steps can be taken to ensure the accuracy and quality of personal information in data systems while guarding against its misuse. From a technical perspective, the challenge is to provide security mechanisms for protecting the confidentiality of individual information used for knowledge discovery and data mining. More specifically, techniques must be developed for replacing original data with data that approximately exhibits the same general patterns, but conceals sensitive information. Mechanisms must be developed that will enable data owners to choose an appropriate balance between privacy and precision.

One option is to use data validation to help guarantee to your application that every data value is correct and accurate. Data validation can be designed into the application with several differing approaches: user interface code, application code, or database constraints. Types of data validation are data type, range checking, code checking, and complex validation.

Governmental entities that employ data systems containing personal information should have publicly-declared privacy policies and develop internal protocols for obtaining and sharing data. In these cases, it is also important to carefully monitor and document data receipt, processing, distribution, utilization, and disposition. Consultation with oversight bodies or dedicated privacy staff is strongly recommended in order to prevent the misuse of personal information in these systems. Procedures for error correction are also important and should be well-publicized, so that no one is forced to live with a mistake in his or her data. Finally, when possible, data-mining programs should have a redress mechanism. Individuals must not only be able to correct database errors, but also, if they are harmed by privacy violations, must be able to take specific legal recourse against the government.

We plan to assess the department's data mining activities in fiscal year 2005, and will address issues concerning protecting privacy rights and personal information as part of that effort.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Norm Coleman

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 1.

In Fiscal Year 2004, St. Paul and Minneapolis received a total of \$20,108,247 in Urban Area Security Initiative Grants. However, this year St. Paul received no money and Minneapolis received only \$5,763,411. It seems to me that if we are to have a coherent homeland security strategy there needs to be consistency in the program not only in terms of funding but in terms of rhyme and reason. Here you have two cities right next to each other that have an interconnected homeland security strategy. One was zeroed out altogether and apparently is to have no homeland security funding while the other was drastically cut. Doesn't a sound homeland security strategy depend on both consistency in terms of funding and policy to avoid wasting money and creating holes in our security?

Answer.

We have not audited the Urban Area Security Initiative (UASI), but we plan to begin an audit of the program this year. That said, the concerns raised in this question are valid. We noted in our Audit of Distributing and Spending “First Responder” Grant Funds (OIG-04-15, March 2004) that one of local governments’ concerns is that they may not have the funds they need to sustain the equipment and level of preparedness they are acquiring. They said that they would like long-term and stable funding. We will look into the consistency issue in our UASI grant program audit.

Question 2.

I have been hearing from law enforcement personnel in Minnesota that the lines of communication between the Department of Homeland Security and local officials still need improvement. From your vantage point, what actions can the Department of Homeland Security take so that the lines of communication are improved and important information is passed along in a timely and effective manner?

Answer.

We have not conducted a review of communications between DHS and local law enforcement officials. However, as part of our review of the proposed merger of CBP and ICE, which we are conducting at Senator Collins’ request, we will be talking to both DHS and local law enforcement field personnel and may gain some insights to this issue.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Norm Coleman

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 3.

With all the emphasis on preparedness in current Department of Homeland Security and Office of Domestic Preparedness guidelines, do you think enough is being accomplished on the Prevention Front? What is your vision for state and local terrorism prevention efforts and how might you suggest dollars be allocated to meet this need?

Answer.

Generally, the people involved with first responder and preparedness grants at the state and local level are more familiar with, and focused on, response activities. Consequently, prevention has received less emphasis than response activities, and the majority of grant funds are being spent on preparedness and response equipment, such as personal protective equipment. Although we have not done work that includes reviewing the balance between prevention and preparedness spending, we believe this difficult and complex issue needs to be carefully considered by DHS. Now that the State Homeland Security, UASI, and the Law Enforcement Terrorism Prevention programs are managed by one office, the Office of State and Local Government Coordination and Preparedness, the Department has an opportunity to focus on the balance between prevention and preparedness.

Question 4.

With regard to student visas, several agencies are involved in determining which foreign students will be allowed to enter the United States to study. What is your view on how these agencies are cooperating with each other and do you think changes need to be made?

Answer.

We have not conducted a review of student visas, and have no basis on which to address the question at this time.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Norm Coleman

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 5.

Currently, when a foreign student wants to apply to school in the United States they need to pay a \$100 SEVIS fee before filling out a visa application. This is separate from the \$100 interview fee. If they are denied a visa, the \$100 SEVIS fee is not refunded. Also, when the student pays the SEVIS fee, they are entered into a database and their name is not removed if they are denied a visa. Do you think that the SEVIS fee process needs to be changed so foreign students are not deterred from applying for a visa and do you think the current management of the database needs to change so we do not have a database full of people that have never set foot on American soil?

Answer.

We have not reviewed visa processing fees, or the management of the related database, and have no basis on which to address the question at this time.

Question 6.

I know that the State Department is working to reverse the decline in student visas. What role can and should the Department of Homeland Security play in reversing perceptions about America being unwelcome to foreign students?

Answer.

We have not conducted a review of student visas, and have no basis on which to address the question at this time.

Question 7.

Currently border security officials located at the northern border of Minnesota and other states have to travel to facilities in Georgia for training. These sites are unable to provide training on how to handle the cold temperatures that border officials encounter on the Canadian border. Have any of you examined whether the Department of Homeland Security should consider adding training facilities in cold weather sites to better train border security personnel there?

Answer.

We have not studied this particular question.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Frank Lautenberg

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 1.

Your written testimony points out that providing qualified and trained [TSA security screener] personnel has been a substantial challenge for TSA (page 8). What specific tasks have the Inspector General’s office taken, are currently underway, or are currently planned, with respect to TSA’s hiring process, techniques, and contract oversight?

Answer.

We have completed several reports, and other work is underway, related to the screener hiring process, screener techniques, and related contract oversight issues, as follows:

1. A review of Background Checks for Federal Passenger and Baggage Screeners at Airports (OIG-04-08, dated Jan. 04)
2. A review of the Use of Alternative Screening Procedures at an Unnamed Airport (OIG-04-028, dated July 04)
3. Audit of Passenger and Baggage Screening Procedures at Domestic Airports (OIG-04-037, dated Sept. 04, SECRET)
4. An Evaluation of TSA’s Screener Training and Methods of Testing (OIG-04-045, dated Sept. 04)
5. Review of TSA Screening Practices in Houston, Texas (OIG-04-048, dated Sept. 04)
6. Review of TSA’s Management Controls over the Screener Recruitment Program (Draft Report in Process, dealing primarily with TSA’s contract with NCS Pearson; expected release in April 04)

Question 2.

TSA is in the process of issuing medical questionnaires to much of its screener workforce, requesting basic information about color perception, visual acuity, physical coordination, motor skills, and auditory abilities. Were such abilities checked by the contractors who were responsible for hiring the screener workforce? Were they required to be checked by contract agreement with the TSA? If not, why not? Beyond report #OIG-04-08, does your office plan to investigate this specific matter of the contract or has your office done any other separate investigation of this matter?

Answer.

Subcontractors checked these abilities during the initial hiring of the screener workforce. These checks were required by TSA's contract with NCS Pearson. We have not done any work specific to this requirement and do not have any planned in fiscal year 2005.

Question 3.

Former Inspector General Clark Kent Ervin has stated that, with respect to TSA security screener effectiveness testing, "the penetration testing we did of [security screening at] airports around the country. Never once did the Secretary seek a briefing from us." Can you confirm this lack of briefing request? Has the Secretary at any time, including the time since Mr. Ervin's departure, requested a briefing from the IG office about the penetration testing?

Answer.

Secretary Ridge did not request a briefing from OIG on the penetration test results, either before or after Mr. Ervin left office. We did brief Under Secretary Hutchinson, at his request.

Question 4.

Has the IG analyzed problems related to TSA security screener retention, or determine whether current agency efforts are sufficient to address retention problems? If so, what tasks have been performed, is the agency doing enough, and what more could be done? If not, does the IG plan to study these issues?

Answer.

We have not analyzed problems related to TSA screener retention, or reviewed current agency efforts to address retention problems. However, TSA has been giving its FSD's more authority to handle personnel matters, and airports that are approved under the opt out program will also have such authority. We plan to look at this issue in FY 2006, once the effect of the new authorities can be assessed.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Frank Lautenberg

"The Department of Homeland Security: The Road Ahead"

January 26, 2005

Question 5.

Has the IG office studied TSA's handling of baggage theft or damage claims? What work has been done, is ongoing, and is planned? What has the IG found with respect to effectiveness of TSA's handling of such claims? Has the IG made any specific suggestions to TSA with regard to their claims processing program? How would the impact of having liability agreements with air carriers impact the effectiveness of the claims process? What would the impact of having security cameras placed in TSA checked baggage screening areas have on the effectiveness of TSA's claims process? Has the TSA or the IG's office identified airport screening locations that are at higher risk of baggage theft/damage, based either on claim data or investigations of screener personnel?

Answer.

On January 11, 2005, we issued a draft report "A Review of Procedures to Prevent Baggage Thefts" to TSA. The objective of our review was to assess the passenger baggage screening process to identify its vulnerabilities for theft. In order to recommend actions that would prevent or diminish baggage thefts, as well as improve loss or stolen baggage claims processing, we analyzed applicable rules and procedures relating to baggage handling and the handling of claims for lost or stolen baggage; interviewed TSA officials from the Claims Management Office (CMO), Office of Internal Affairs and Program Review (OIPR), Office of Human Resources, and four major airports; observed checked and carry-on baggage and passenger checkpoint screening processes at Ronald Reagan Washington National airport, Baltimore Washington International airport, John F. Kennedy International airport, and LaGuardia International airport; and interviewed officials from two large commercial airlines and contacted an airlines' passenger advocacy group to obtain their assessment on the extent of the baggage theft issue.

Our report contains recommendations regarding preventive measures and claims settlements. We expect to issue it shortly.

Question 6.

Has the IG office performed any analysis of TSA's efforts to establish staffing standards for aviation security screeners?

Answer.

Generally, TSA's hiring standards, including such things as physical and language abilities, were established in ATSA. TSA's initial decisions on the number of screeners at individual airports were based largely on general staffing models and congressional restrictions on total screeners. While we have not specifically analyzed the standards, our work has shown that the hiring standards resulted in a very high rejection rate for screener applicants, significantly increasing recruitment costs, and officials at many airports have complained of insufficient numbers of screeners.

Question 7.

Has the IG analyzed the TSA's delegation of authority to Federal Security Directors (FSDs) concerning screener personnel decisions, including hiring and dismissal? If so, what has your office found? In your opinion, do FSD's have adequate resources to effectively manage the workforces they are responsible for? If not, what more is necessary?

Answer.

We have not analyzed TSA's delegation of authority to FSDs concerning screener personnel decisions. We plan to look at aspects of FSD authorities and coordination with airport stakeholders later this year.

Question 8.

Former FSD Tony Zotto from Ronald Reagan Washington National Airport has stated that because FSD's aren't sworn law-enforcement officers, they can be excluded from police and intelligence briefings. Do you feel that TSA has processes and procedures in place to ensure that FSD's are provided with intelligence information relating to aviation security in a timely manner?

Answer.

We have not received similar complaints from other FSD's and have not had reason to examine the question. In considering the use and exchange of law enforcement information within TSA, however, the information gathering, analysis, and dissemination performed by the Transportation Security Intelligence Service, the National Targeting Center, and the Transportation Security Operations Center appear relevant to your question.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Frank Lautenberg

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 9.

Your testimony cites only the lack of memoranda of understanding between TSA and various DOT agencies as a major concern in the area of rail and transit security. What efforts has your office undertaken, are ongoing, and are planned, with respect to oversight of the Department's efforts to secure rail and transit facilities and operations? Do you feel that the Department has adequate direction in its mission to address rail and transit security needs?

Answer.

There is now a memorandum of understanding (MOU) between DHS and DOT. DHS and DOT are developing annexes to the MOU to address roles, responsibilities and resources.

Our office is currently reviewing TSA's efforts to improve the security of mass transit systems in major metropolitan areas. TSA's efforts to date have been directed toward identifying critical system assets such as rail and subway stations, command and control centers, and communication stations. TSA will then conduct vulnerability assessments on the most critical or nationally important assets to identify potential areas of weakness against plausible threats and protective measures to mitigate the weakness. For the assets less critical or not nationally important, local transit agencies can use a self-assessment tool developed by TSA to assess their vulnerability.

Question 10.

The FY 2005 Homeland Security Appropriations Act provided funding for the hiring of rail security inspectors. What is the labor market for such inspectors? In your opinion, do DOT agencies such as the Federal Railroad Administration stand to lose experienced safety inspectors who choose to work for DHS?

Answer.

We have not reviewed the hiring of rail inspectors, and have no basis on which to address these questions.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Frank Lautenberg

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 11.

From an operational perspective, what qualifications and experience do you feel the DHS Inspector General must possess in order to effectively carry out the responsibilities of the position?

Answer.

The Inspector General Act of 1978, as amended, 5 U.S. C. Appendix 3, provides that the Inspector General “shall be appointed by the President, by and with the advice of the Senate, without regard to political affiliation and solely on the basis of integrity and demonstrated ability in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations.” In addition to those statutory prerequisites, the Inspector General (IG) must be a firm believer in the IG concept and its mission and passionate about its independence.

That said, an effective IG must be:

- Knowledgeable – both internally and externally. This requires that the IG keep abreast of departmental programs and operations.
- Collaborative – the IG must be able to work together with departmental leadership to identify the most important areas for OIG work, and identify the best means of addressing the results of that work, with consideration of the Department’s point of view while maintaining the OIG’s statutory independence. The IG must be fair and balanced at all times. This requires that the IG maintain an open line of communication – both internally and externally, both formally and informally, and frequently. The IG must keep Department heads and Congress informed of problems at the earliest possible time.
- Collegial – disagreements should not cause relationship with management to become unproductive. The IG and departmental leaders share a common goal: the successful accomplishment of the Department’s mission.
- Proactive – to the extent possible, serve as a management consultant/advisor on new Departmental initiatives. Where practical, prevent problems before they occur.

Bottom line – The IG’s primary mission is to support the Secretary, and the Congress by promoting economy, efficiency, and effectiveness within the Department; and preventing and detecting fraud, waste, and abuse in departmental programs and operations.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Frank Lautenberg

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 12.

Does the U.S. Coast Guard possess the resources it requires to maintain sustained high operating tempo? What is at risk should the Coast Guard be unable to maintain its level of performance at this tempo?

Answer.

It is unclear at this time --pending completion of the Department's review of the Integrated Deepwater System plans which may effect the Coast Guard's AC&I and O&S budgets--whether the Coast Guard possesses the resources required to maintain sustained high operating tempo. As noted in our September 2004 report on Coast Guard Mission Performance, continued high operating tempo will wear down assets faster than previously planned, requiring additional maintenance, repair, or replacement of engines and other components that wear with use. The aging Coast Guard surface and aviation fleet is deteriorating, putting the Coast Guard's ability to balance its missions, maintain performance of its homeland security missions, restore the performance level of its non-homeland security missions to their pre-September 11th levels, and—most significantly—jeopardizing the readiness and capacity of the Coast Guard to surge operations in response to a major crisis or increased threat level.

As is noted in the Department's FY 2006 budget request, it is reviewing, with the objective of revising, the Integrated Deepwater System program plans. The current Integrated Deepwater System program baseline is outdated and needs to be updated to post-September 11th operating tempos and requirements. The results of this review are to be provided the Congress upon completion.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Frank Lautenberg

"The Department of Homeland Security: The Road Ahead"

January 26, 2005

Question 13.

Your office identified the port security grant program as lacking direction, or a priority basis on which to make grant awards. As a result of this, can you quantify the harm to the vulnerability of our nation's maritime system to terrorism? If not, what are the implications of a lack of clear security priorities for homeland security grant programs such as this?

Answer.

Despite the existence of well-conceived evaluation criteria on which to base grant award decisions, the manner in which the program evaluated and selected projects hindered its strategic effectiveness. The possibility of harm to the vulnerability of the nation's maritime system is not easily quantified. In terms of the actual grant awards, the program funded several hundred questionable projects in rounds two and three. In addition, ODP awarded approximately \$70 million in grants for projects it received from TSA's pool of applications that the TSA, USCG, and MARAD national review board determined did not merit funding.

The most significant question for sector-specific grants programs like port security is whether they can be designed to strategically protect nationally critical infrastructure and key assets. This program's strategic effectiveness is hindered because it is attempting to reconcile three competing approaches: the competitive program mandated by Congress, MTSAs grant authority, and risk-based decision making. The program is under pressure to help defray the costs of the MTSAs security mandates that broadly affect the maritime industry. Moreover, the program's ability to focus its resources on the nation's most critical port infrastructure is limited because it can only base award decisions on the universe of applications submitted. In addition, the evaluation and selection process has emphasized disbursing grant awards to many applicants. Hence, the program attempts to balance the competitive program that objectively evaluates the quality of the applications with the need to broadly disburse funds to assist with MTSAs compliance, while at the same time incorporating risk-based eligibility criteria and evaluation tools to prioritize projects. The competing approaches have clouded the direction of the program; its purpose and goals need to be refined.

In its response to our draft report, DHS said that it would redesign the program to emphasize risk-based decision-making that is "sensitive" to MTSAs mandates. DHS may discontinue the program as a stand-alone program. The Administration proposed in its FY 2006 Budget Request to merge the program with other transportation-related grant programs into a new Targeted Infrastructure Protection Program. As this program unfolds, DHS would be well served to integrate its port security grant program with IAIP's national critical infrastructure protection initiatives and the USCG's efforts to identify and prioritize the nation's most critical port infrastructure.

Post-Hearing Questions for the Record
Submitted to Richard L. Skinner
From Senator Frank Lautenberg

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

Question 14.

The northern New Jersey area contains, according to the FBI, “most dangerous two miles in the United States when it comes to terrorism” and was under an Orange threat level from August 1st to just after the Presidential election. In light of this, funding in the Urban Area Security Initiative, a program for high threat urban areas, was cut for Jersey City’s homeland security funds will drop by 60 percent, from \$17 million in FY 2004 to \$6.7 million in FY 2005. Newark will see a 17 percent reduction in funds, from \$14.9 million to \$12.4 million, while 10 other cities throughout the country received more funding than Newark and Jersey City and saw an increase in funding from last year. Do you think the current distribution of funding is the best way in providing resources for at risk areas? Do you think the Department should revise its formula in distributing the UASI grant?

Answer.

We have not reviewed the UASI program, but have plans to do so later this year. We have no basis on which to comment on funding distribution at this time.

Post-Hearing Questions for the Record
Submitted to James Jay Carafano, Ph.D.
From Senator Susan Collins

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

1. Given the wide range of activities over which the Department of Homeland Security has influence, it is essential that DHS coordinate its activities with other federal agencies. For example, bioterrorism responsibilities are divided between HHS and DHS. Do you think this division has worked to date, and if not, how do you think these responsibilities should be reallocated?

Answer: This is actually an issue I am just beginning to study. The Heritage Foundation is in the process of establishing a working group to examine issues related to medical responses to catastrophic terrorism. I would be happy to come brief you or your staff after the working group concludes its study.

Our preliminary research suggests the following. The current federal response system is predicated on the thoughtful and systematic application of resources. Local communities are expected to deal with disasters and emergencies using their own resources. When they lack adequate capacity, they call on the assets from the state and neighboring jurisdictions. Federal resources are brought to bear only after state and local governments find they lack adequate capacity and request assistance from the federal government. In turn, FEMA then has to determine the level of required assistance and then coordinate the delivery of support with HHS, the DOD, the VA, and other federal agencies. The current approach could well prove totally inadequate in the event of a virulent biotoxin attack. Effectively negating threats in many cases requires a rapid response capability, and operating on compressed timelines leaves little room for delayed delivery of support or missteps in coordination.

The Department of Homeland Security (DHS) lacks the expertise and experience to oversee large medical emergency response programs. The Metropolitan Medical Response System, and the National Disaster Medical System should be overseen by the Department of Health and Human Services.

However, to improve the DHS coordination role in medical response more can be done. To improve coordination of the national bioterrorism response effort and ensure that key biomedical response programs are seamlessly integrated into the overall national response system, the DHS requires a level of management commensurate with the assistant secretaries providing oversight for the DOD, VA, and HHS. Congress should establish an Assistant Secretary for Bioterrorism

and Infectious Disease Response. The Assistant Secretary should have responsibility for ensuring that plans and programs under development--including the National Response Plan, National Incident Management System, and HHS national preparedness plan--are consistent and provide for the rapid delivery of services and support in the event of biomedical emergency.

2. Are there adequate plans for the medical response to a bioterrorism attack, and are these plans the product of adequate coordination between DHS and HHS?

Answer: I don't think so. Our preliminary research raises one particular area of concern. Additionally, The federal government lacks an integrated approach to emergency medicine, a key component for responding to a bioterrorist attack. HHS, for example, does not have a National Institute of Emergency Medicine. The Emergency Medical Services Division, tasked with developing the federal contribution to enhancing and guiding the emergency medical system, is a small office within the Department of Transportation's National Highway and Traffic Safety Administration, far removed from other key elements of the federal emergency medical response system in HHS and DHS.

Congress should amend the Public Health Security and Bioterrorism Preparedness and Response Act and address the shortfall in federal expertise in emergency medical services, including moving Emergency Medical Services Division functions to HHS and establishing an Institute for Emergency Medicine as part of the National Institutes of Health, dedicated to spearheading emergency medical research efforts. This institute should work closely with the CDC to devise more comprehensive emergency medical response strategies.

3. During the 1990s, the Justice Department developed two different, incompatible fingerprint screening programs – IDENT was developed by the INS, and IAFIS was developed by the FBI. It has been a challenge for years to integrate these programs, a challenge made more difficult by moving the IDENT program over to DHS. The integration of these systems is critically important, especially given the fact that US-VISIT uses the IDENT system. Are these systems compatible, and if not, what will it take to make them compatible?

Answer: I think more needs to be done, but forcing the DHS to conform to the FBI system as suggested by the recent Department of Justice Inspector General report is simply the wrong answer. I applaud the administration's effort to create a new Screening Coordination and Operations Office in DHS to oversee the various DHS programs. The office should prove a more effective partner in the interagency process of ensuring that various government systems are compatible.

4. Can you comment on DHS's progress with the development and deployment of biometric identification systems in general and TWIC in particular? How do you view the priority they have given this program, more than three years after 9/11 ?

Answer: My concern with regard to these programs are the typical concerns of any federal program that involves deploying new identity systems and Information Technologies (IT). Appropriators need to pay particular attention to homeland security programs with significant IT components. The federal government's track record in developing IT networks is checkered at best. Programs that lack senior leader involvement, well-developed enterprise architectures, appropriate management and contractual oversight, and effective risk-mitigation strategies often find that results fail to meet expectations or that IT costs balloon out of control--crowding out funding for other critical operational needs. The Department of Homeland Security is no exception. The DHS Inspector General has already warned that IT management represents a major challenge for the department.

Again, I applaud the administration's effort to create a new Screening Coordination and Operations Office, which hopefully will provide better oversight of programs like TWIC and ensure their integration with other federal initiatives. Still, Congress must watch these efforts closely. Congress should establish specific guidelines and reporting requirements in budget authorization legislation.

5. Can you discuss how DHS should ensure the interoperability and compatibility of the various biometric identification systems that have been deployed and are being developed by DHS and other agencies?

Answer: Again, I think the Administration's effort to create a new Screening Coordination and Operations Office is a step in the right direction. For further information, please see "Biometric Technologies: Security, Legal, and Policy Implications" available at www.heritage.org/Research/HomelandDefense/lm12.cfm.

6. In general, have DHS activities in the areas of technology development, preparedness, and intelligence been adequately coordinated with other federal agencies? If not, what recommendations would you make to improve this coordination?

Answer: My major concern is the lack of fully exploiting the potential for collaboration between the DHS and the Department of Defense. More cooperation is called for in the development and acquisition of future technologies that are mutually critical to defense and homeland security. Research suggests there are significant opportunities for collaboration. On the other hand, few initiatives appear underway. Much current cooperation is through the Technical Support Working Group, but these efforts focus on commercial off-the-shelf technologies, not long-term research and development. I addressed this issue in some depth as part of a research project conducted by the National Academies of Science and I would commend its report to the committee. See, Board on Army Science and Technology, Army Science and Technology for Homeland Security, vol. 2. (Washington, DC: National Academies of Science Press, 2004). DOD is currently drafting its homeland defense strategy. This strategy will likely determine the future course of cooperation between the departments. Further progress will likely be limited until the strategy is published or new guidance is provided in the DOD's 2005 Quadrennial Defense Review.

Post-Hearing Questions for the Record
Submitted to James Jay Carafano, Ph.D.
From Senator Norm Coleman

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

1. In Fiscal Year 2004, St. Paul and Minneapolis received a total of \$20,108,247 in Urban Area Security Initiative Grants. However, this year St. Paul received no money and Minneapolis received only \$5,763,411. It seems to me that if we are to have a coherent homeland security strategy there needs to be consistency in the program not only in terms of funding but in terms of rhyme and reason. Here you have two cities right next to each other that have an interconnected homeland security strategy. One was zeroed out altogether and apparently is to have no homeland security funding while the other was drastically cut. Doesn't a sound homeland security strategy depend on both consistency in terms of funding and policy to avoid wasting money and creating holes in our security?

Answer: I agree with you. This makes no sense. Merely disbursing funds to meet many demands risks spending a little on everything and not providing much security for anything. Investing in the wrong priorities can be equally troubling. Congress and the Administration cannot address homeland security funding in a piecemeal fashion. Congress and the administration should agree on a set of strategic guiding principles that will allow smart spending to replace more spending.

The solution to this problem is establishing national performance standards, a framework for spending based on strategic needs, not stakeholder interests, and a consistent, predictable funding stream. Here is what I recommend.

The highest priority for federal spending must be investments that assist in creating a true national preparedness system—not merely supplementing the needs of state and local governments. Washington's greatest responsibility in building a national system is accomplishing the unique roles and missions that belong to the federal government, duties that *are not* the primary concern of state and local governments and the private sector. The administration has two key responsibilities in this area and the budget reflects both priorities.

- *The federal government is primarily responsible for stopping foreign terrorists before they attack our citizens.* Thus, activities that disrupt or prevent terrorist acts should receive the highest priority. In the FY2006 budget proposals these initiatives comprise the lion's share of total domestic security spending, 57 percent, a two percent increase over FY 2005.

- *The federal government is also primarily responsible for protecting its own critical infrastructure.* This priority is also reflected in the FY2006 budget proposal. Of the \$22.7 billion homeland security spending outside the DHS, \$12.8 billion is for critical infrastructure programs. This represents a total of 57 percent of all domestic security spending by the other federal departments and agencies.

After seeing to its own responsibilities, the federal government properly has the task of constructing the national system that will allow state and local governments and the private to participate in an effective domestic national security network. That includes providing state and local governments with the capability to integrate their counterterrorism, preparedness, and response efforts into a national system; and expanding their capacity to coordinate support, share resources, and exchange and exploit information. In addition, the federal government must enhance its own capacity to increase situational awareness of national homeland security activities and to shift resources where and when they are needed.

Simply giving states and local governments money to increase their capacity to respond to a terrorist attack is the wrong answer. Such an approach won't help build a national system. Additionally, the dollars that might be needed to equip every state and U.S. territory with sufficient resources to conduct each critical homeland security task could run into the hundreds of billions. Although the federal government has a responsibility to assist states and cities in providing for homeland security, it cannot service every one of their needs. Indeed, state and local governments are having difficulty absorbing and efficiently using the federal funds that are already available.

A hallmark of the president's proposed FY 2006 budget is the restraint demonstrated in providing grants to state and local governments and efforts to restructure DHS grants to focus them on strategic needs rather than a fixed allocation to individual states. The administration proposes to allocate \$3.4 billion in grants, a reduction from the \$3.6 billion allocated in FY 2005. The budget also calls for HHS to distribute a total of about \$1.3 billion in grants assistance to improve state and local health services and hospital preparedness. In total of the budget allocates \$4.7 billion in spending homeland security assistance, a reduction of about 6 percent.

Additionally the administration proposes to restructure \$2.6 billion in grants. The restructuring includes reducing the minimum allocated to each state .25 percent of total funds allocated for the State Homeland Security Grant Program (proposed \$1 billion), instead of the current minimum of .75. The administration also proposes consolidating the Law Enforcement Terrorism Program into the state program and transferring part of the Urban Area Security Initiative grants and port, transit system and other infrastructure grants into a Targeted Infrastructure Protection Program.

Given that the administration has not fully implemented Homeland Security Presidential Directive 8, (HSPD-8) which would establish national preparedness standards and improve the allocation of grants by more clearly distributing funds based on concrete threat and vulnerability assessments, and that Congress has failed to pass legislation that would require grants be allocated by strategic needs, the administration is right to restrain the amount of funds allocated to state and local governments.

No additional earmarks should be made for homeland security grants. Congress should reframe from throwing money at the problem. In fact, the Congress could strengthen the administration's effort to strategically target funding by eliminating Assistance to Firefighter Grants (Fire Grants) and reallocating these funds (proposed \$ 500 million) to the general State Homeland Security Grant Program. The Fire Grant program principally benefits rural communities and does nothing to contribute to building a national homeland security network. Funds could be much more effectively employed for other purposes.

In addition, Congress could help make the process of a building a national preparedness system not by increasing funding for preparedness and emergency response, but by (1) passing legislation which would essentially put HSPD-8 into law and (2) reorganizing the Department of Homeland Security (DHS) so that it could more efficiently oversee the components of the department managing its efforts to develop an efficient national preparedness system. The Congress should consolidate DHS critical infrastructure protection, preparedness, and state/local/private coordination efforts under an Undersecretary for Protection and Preparedness. This would consolidate the following agencies, components, and authorities: (1) the Infrastructure Protection component of the Information Analysis and Infrastructure Protection Directorate; (2) the Office of State and Local Government Coordination and Preparedness; (3) the non-operational transportation infrastructure protection mission of Transportation Security Administration (TSA); (4) the "preparedness" piece of the Emergency Preparedness and Response Directorate; (5) the private sector preparedness mission of the Office of Private Sector Liaison; and (6) DHS grantmaking authority. Consolidating these disparate efforts would provide the DHS Secretary with a stronger platform from which to lead national efforts to build a true national preparedness system.

2. I have been hearing from law enforcement personnel in Minnesota that the lines of communication between the Department of Homeland Security and local officials still need improvement. From your vantage point, what actions can the Department of Homeland Security take so that the lines of communication are improved and important information is passed along in a timely and effective manner?

Answer: The first has to be to establish a regional framework for the Department of Homeland security (DHS). Although state and local officials will undoubtedly lead the initial response to any crisis, it is improbable that a major terrorist attack would affect only a single city or that a single municipal authority would have sufficient assets to manage such a calamity alone. At a minimum, response efforts would likely require mutual aid from multiple jurisdictions. In a major crisis, federal assets would supplement state and local resources. Effective cooperation among officials at all levels of government and the private sector is essential, yet the DHS lacks an adequate regional structure to facilitate coordination.

Whatever regional security structure the Administration decides to support, the DHS should implement the proposal in a way that allows stakeholders an opportunity to participate in the process to a greater extent than has been the case to date. Through speeches, publications, and other media events, DHS representatives should first announce the principles for regional design that underpin their recommendations. Stakeholders should then be allowed time to comment on them through formal and informal mechanisms. Ideally, such an interactive process would result both in a better proposal and in stakeholders' becoming more committed to the subsequent reorganization.

The first priority of this regional organization should be to support the flow of information and coordinate training, exercises, and professional development for state and local governments and the private sector. The structure's key operational mission should be to enhance prevention, preparedness, response, and critical infrastructure protection at the regional level, as well as to coordinate activities like intelligence sharing and early warning with the Justice Department's regional Joint Terrorism Task Forces (JTTFs).

As a secondary priority, the DHS regional framework could achieve cost savings and other efficiencies by highlighting regional redundancies and promoting consolidations across geographic boundaries. The July 2002 National Strategy for Homeland Security called for enhanced cooperation among actors at the various levels of government and the private sector to avoid duplication and better integrate scarce national homeland security assets. Obvious candidates for improved regional integration of support functions include IT systems and administrative activities.

Third, regional offices could better integrate the homeland security programs of state and local entities, both public and private, with DHS policymakers in Washington. Serving as conveniently located points of contact for state, local, and private actors, regional coordinators could assume a lead role in identifying the needs and resources that exist both nationally and within their regions.

Regional offices should also improve situational awareness and transparency among homeland security actors by promoting information sharing among them. Increased data exchanges could occur both electronically, through an expansion of the horizontal communication provided by the Joint Regional Information Exchange System (JRIES) and related networks, and through additional opportunities for personal encounters. People involved with homeland security at the state and local

levels—including first responders, public health experts, and law enforcement officials—have diverse backgrounds and expertise, so their approaches to these issues (as well as their insights regarding them) likely differ. State-level actors in particular could benefit from more frequent interaction with their nearby colleagues given that many crises could easily spill across state boundaries.

A second step must be to implement the initiatives established by the Intelligence Reform and Terrorism Prevention Act of 2004. In particular, the law mandated that the president establish an “information sharing environment” (ISE) to distribute intelligence regarding terrorism to appropriate federal, state, local and private entities. Section 1016 of the law requires designating an organizational and management structure to establish and maintain the ISE and report back to Congress within one year on the plans for implementation. The law also called for creating an Information Sharing Council to advise the president and the ISE program manager on developing policies, procedures, guidelines, roles, and standards for establishing and maintaining the ISE.

Over the long-term, the ISE could provide critical capabilities for enhancing the role of state and local agencies in counterterrorism operations. To ensure that they appropriately access and contribute to the ISE, state and local representatives should be given key positions in the Information Sharing Council to ensure that their needs and potential contributions are adequately addressed.

3. With all the emphasis on preparedness in current Department of Homeland Security and Office of Domestic Preparedness guidelines, do you think enough is being accomplished on the Prevention Front? What is your vision for state and local terrorism prevention efforts and how might you suggest dollars be allocated to meet this need?

Answer: No, I think much more could and should be done. State and local governments have a critical role to play in combating terrorism. However, too much emphasis has been placed on preparing them to respond to terrorist acts and not enough attention has been paid to enhancing their ability to prevent attacks on U.S. citizens. The Department of Homeland Security (DHS) should address this imbalance by establishing a national program aimed at enhancing state and local capacity to fight terrorism. The program should focus on improving information analysis capabilities, strengthening the means of state and local law enforcement to conduct terrorism-related immigration investigations, maintaining strong legal authority for information sharing, and establishing a template for state intelligence operations. Any national effort must respect the principles of federalism both in what the federal government can ask of the states and states' responsibilities. DHS should implement this program with support from the Department of Justice (DOJ). Establishing an agenda for these efforts ought to be one of the first priorities for the new Secretary of Homeland Security.

4. With regard to student visas, several agencies are involved in determining which foreign

students will be allowed to enter the United States to study. What is your view on how these agencies are cooperating with each other and do you think changes need to be made?

Answer: I strongly believe that all visa activities should be consolidated in a single federal agency.

Under the Homeland Security Act, responsibility for ensuring that terrorists do not obtain visas to enter the United States is shared by DHS and the State Department's Bureau of Consular Affairs. This has led to a significant turf struggle. Indeed, the process of negotiating a memorandum of understanding between the State Department and DHS delineating their respective responsibilities took over one year. Additionally, there has been policy paralysis, even as many observers have viewed post-9/11 U.S. visa policy as a disaster—with security trumping all other objectives and deterring many individuals who present no threat from seeking to come to the U.S. or tying them up in excessive bureaucratic delays. The problems associated with post-9-11 visa policy, because of their impact on economic, diplomatic, academic, and scientific exchanges, have the potential to undermine long-term security interests.

Congress should consolidate responsibility for visa operations within a single federal agency. Splitting responsibility for visa issuance and management between DHS and the State Department was a mistake. Operations could be managed more efficiently under one department and would place responsibility and accountability in one place. The choice is difficult. Arguably, the State Department is better positioned to consider the diplomatic, economic, and cultural issues at stake in issuing visas. On the other hand, if DHS were responsible, it would be better able to seamlessly integrate visa management into its other border control responsibilities and coordinate visa operations with its other international responsibilities.

5. Currently, when a foreign student wants to apply to school in the United States they need to pay a \$100 SEVIS fee before filling out a visa application. This is separate from the \$100 interview fee. If they are denied a visa, the \$100 SEVIS fee is not refunded. Also, when the student pays the SEVIS fee, they are entered into a database and their name is not removed if they are denied a visa. Do you think that the SEVIS fee process needs to be changed so foreign students are not deterred from applying for a visa and do you think the current management of the database needs to change so we do not have a database full of people that have never set foot on American soil?

Answer: I think the a non-refundable fee is a deterrent to people who should not be applying in the first place and I think visa issuance is pay-for-service activity. Applicants are paying for having their application processed, not paying to get a visa.

There is utility in keeping a record of those individuals who applied for student visas and were rejected. Maintaining such a database does raise some privacy concerns, though fewer than if the database held information on U.S. persons. In any case, such concerns can be mitigated by ensuring that appropriate privacy protocols are in place.

6. I know that the State Department is working to reverse the decline in student visas. What role can and should the Department of Homeland Security play in reversing perceptions about America being unwelcome to foreign students?

Answer: If there is a role for DHS in changing perceptions of the U.S., the Office of International Affairs would be the best place for such a responsibility. Unfortunately, with its current funding, the office would not be able to contribute much to altering such perceptions.

This issue reflects a larger problem with the role of the DHS in international affairs. Although DHS has established an Office of International Affairs (OIA) to set strategic direction for the department's international activities, DHS international efforts remain fragmented among multiple offices, including the OIA, the Border and Transportation Security's (BTS) Policy Office, and other agency policy and operational activities within Immigration and Customs Enforcement (ICE), Citizenship and Immigration Services (CIS), Customs and Border Protection (CBP), and the U.S. Coast Guard. Because of this fragmentation (which reflects DHS's overall incomplete integration), DHS is unable to present a unified effort and presence overseas. As a result, DHS remains disenfranchised from the foreign policy apparatus. Within embassies, DHS presence is ad hoc and its role, mission, and relationship with the rest of the embassy is unclear. Foreign governments that share security interests with the U.S. may fail to build effective partnerships because of the lack of a clear path to partnership. I would address this issue by establishing an Undersecretary for Policy in the DHS with an Assistant Secretary for Policy (International Affairs).

7. Currently border security officials located at the northern border of Minnesota and other states have to travel to facilities in Georgia for training. These sites are unable to provide training on how to handle the cold temperatures that border officials encounter on the Canadian border. Have any of you examined whether the Department of Homeland Security should consider adding training facilities in cold weather sites to better train border security personnel there?

Answer: I think this proposal may have some merit, but it should be considered as part of a broad review of border security policy. The administration and the Congress still lack the knowledge and mechanisms to determine where to make appropriate investments and effective trade-offs regarding border security. Too often the debate over where to invest in improving security has focused on spending on the border and ports of entry into the United States. The metric of success, however, is not how much money is spent on border and transportation security at the point where people and goods enter the country, but how much is being done to limit the illegal entry into and unlawful presence in the United States.

Stopping the transit of bad people and things is a problem that has been considered from the origin of illicit activity origin to its final destination. Investments need to be made on

initiatives that best disrupt the travel of terrorists and other criminal activities. In this regard, the highest pay-off investments are not necessarily on the border or at ports of entry. For example, while the United States does need to strengthen border security, this should not be done at the expense of internal enforcement, which is perhaps more likely to significantly contribute to reducing illegal entry and unlawful presence more than simply adding border guards. In that respect, the administration was right to eschew the call from Congress in the Intelligence Reform and Terrorism Prevention Act of 2004 to hire thousands of additional border guards in favor of a more balanced investment in additional border security measures and an increased capacity to support detention and removal of individuals unlawfully present in the United States and the prosecution of immigration cases.

Undoubtedly, more needs to be done to address the flow of bad people and bad things across America's borders. But before the Congress puts more money into this area, the administration needs a better blueprint on how to spend the money effectively. DHS must conduct a national assessment of the resources required for effective border security, including all the layers of security that impact securing the border. This analysis should be used to help Congress and the Administration determine where to direct resources to ensure that funding is directed toward programs that provide the greatest contribution to supporting the critical border security mission.

In the meanwhile, Congress can insist on organizational improvements within DHS that will enable the department to deliver more bang for the buck. This is particularly important in the area of border and transportation security where the department is saddled with an inefficient organization that splits responsibilities for border security and internal enforcement. The split of responsibilities between Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) was done without a compelling reason—other than the vague descriptive notion that CBP would handle “border enforcement,” and ICE would handle “interior enforcement.” Indeed, in various interviews, not one person has been able to coherently argue why CBP and ICE were created as separate operational agencies.

Congress should rationalize border security and immigration enforcement by merging CBP and ICE eliminating the Directorate of Border and Transportation Security (BTS). BTS has neither the staff nor infrastructure to integrate the operations of CBP and ICE on a consistent basis—outside the occasional task force, like the Arizona Border Control Initiative. Merging CBP and ICE will bring together under one roof all of the tools of effective border and immigration enforcement: Inspectors, Border Patrol Agents, Special Agents, Detention and Removal Officers, and Intelligence Analysts—and realize the objective of creating a single border and immigration enforcement agency.

Post-Hearing Questions for the Record
Submitted to James Jay Carafano, Ph.D.
From Senator Daniel Akaka

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

1. Your report discusses the importance of international affairs in DHS's activities. As you stated, the current Office of International Affairs in DHS has not lived up to its intended vision for a number of reasons, not the least of which is funding. It has been argued by members of the individual directorates that their international operations must be coordinated separately, and consolidation into an Assistant Secretary position, as you suggest in your report, would hinder their work. Will you address this concern and elaborate on how you envision coordination between an Assistant Secretary for Policy (International Affairs) and the international components of the various agencies?

Answer: I think the key is to establish the office at a sufficiently high level with the DHS secretariat and assign it appropriate responsibilities. I would establish and clearly delineate the key responsibilities of the Assistant Secretary for Policy (International Affairs). They should include: (1) coordinating policy regarding international activities among DHS agencies; (2) coordinating international visits of the secretary related to protocol issues, and (3) ensuring DHS representation in dealing with international institutions, including the United Nations, NATO, the EU, the International Maritime Organization, and the World Customs Organization.

2. Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) personnel have expressed their concerns to me regarding the seemingly arbitrary manner in which the Immigration and Naturalization Service was split between CBP and ICE. The result has been mismanaged budgets, which prompted a hiring freeze for CBP and ICE in the spring of 2004, an ongoing overall budget freeze for ICE, and low staff morale. In your report, you suggest the merging of CBP and ICE. Did the taskforce identify any drawbacks to such a merger and was the recommendation unanimous?

Answer: The task force did not identify any specific drawbacks. Like any merger, there will be a period of transition while all of the details are worked out. While there may be drawbacks to merging CBP/ICE, the task force felt that they would be less of a concern than the current arrangement.

3. In your report, you suggest that visa operations should be consolidated into one federal agency, either at the State Department or DHS. However, the report does not recommend one department over the other. Would you share with the Committee the department that you believe is best suited to carry out this critical function?

Answer: While the Homeland Security Act of 2002 gave the Secretary of the DHS exclusive authority to issue regulations and administer the visa program, consular officers remained part of the Department of State. This was a mistake. For the DHS to fulfill its responsibilities in the visa process, and because of the national security aspect of visa approvals, the Bureau of Consular Affairs' Office of Visa Services should be placed under the DHS. Moving the Visa Office to the DHS would enable the DHS to focus on tightening, improving, and more broadly utilizing the visa function to meet the exigencies of homeland security.

4. Since the creation of DHS, employee morale has been of great concern. Employees are fearful of the new human resources system and the erosion of their rights. They are also concerned about their ability to do their jobs effectively due to the internal organization of the Department. As employee morale can affect recruitment and retention efforts, as well as the agency's mission, what recommendations do you have for improving employee morale and improving the Department's relationship with employee groups?

Answer: Establish an executive leadership program. Higher priority must be given to establishing leader and personnel development programs for a more homogeneous and unified workforce across the department, both in terms of building a shared DHS culture and in developing the skills and attributes required to deal with the challenges of the 21st century. The department needs something similar to the requirements established for the Department of Defense by the Goldwater-Nichols Act of 1986, which prescribed education, interagency and interdepartmental assignments, and skill levels for senior leaders.

5. According to a report I requested from the Government Accountability Office on government data mining activities that was issued last May, the Department of Homeland Security had 11 data mining systems either planned or in operation, not including CAPPS II or its successor Secure Flight, that use personal information. Four of those systems use information from the private sector and eight of them use information from other government agencies.

- In your opinion, what is the best way to ensure that the use of personal information in data mining systems is not running afoul of privacy rights and protections?
- How do we ensure the accuracy and quality of the mined data and how do we prevent its misuse?

Answer: Too much of the debate over the role of information technology in counterterrorism--particularly around the role of commercial databases--has consisted of unsubstantiated claims of utility or non-specific fears of abuse. In

order to make progress in improving the nation's response to terrorism and preserving civil liberties, it is necessary to assess carefully what uses of information technologies will be effective in fighting terrorism, what their impact on civil liberties will be, and how any adverse impacts can be avoided. To achieve this, we need dialogue and consultation between those designing the technologies and those framing the policies for their use. We also need to examine the information practices of the private sector, which has experience operating under constraints on the use of information that are in some respects more stringent than those applicable to law enforcement and intelligence agencies. And we need to draw on academic research to identify emerging technologies that can overcome privacy concerns.

In considering whether to implement new technologies that share, analyze, and correlate disparate data (sometimes called "data mining" or "knowledge discovery") in aid of efforts to prevent terrorism, are there ways to design and implement the technology to affirmatively protect privacy? In particular, we will examine three solutions that have been put forth: (1) anonymization techniques that allow data to be usefully shared or searched without disclosing identity; (2) permissioning systems that build privacy rules and authorization standards into databases and search engines; and (3) immutable audit trails that will make it possible to identify misuse or inappropriate access to or disclosure of sensitive data. We think that each has promise and that further careful research regarding them might contribute to the development of tools for enhanced information analysis that simultaneously protect individual privacy. In other words, security and privacy need not be traded off. The current crisis facing America might not require a zero-sum response.

A colleague of mine, Paul Rosenzweig had these suggestions with regard to the Total Information Awareness program:

The technology can be developed in a manner that renders it effective, while posing minimal risks to American liberties, if the system is crafted carefully, with built-in safeguards that act to check the possibilities of error or abuse. In summary they are:

- Congressional authorization should be required before data mining technology (also known as Knowledge Discovery (KD) technology) is deployed;
- KD technology should be used to examine individual subjects only in compliance with internal guidelines and only with a system that "builds in" existing legal limitations on access to third-party data;
- KD technology should be used to examine terrorist patterns only if each pattern query is authorized by a Senate-confirmed official using a system that: a) allows only for the initial examination of government databases, and b) disaggregates individual identifying information from the pattern analysis;

- Protection of individual anonymity by ensuring that individual identities are not disclosed without the approval of a federal judge;
- A statutory or regulatory requirement that the only consequence of identification by pattern analysis is additional investigation;
- Provision of a robust legal mechanism for the correction of false positive identifications;
- Heightened accountability and oversight, including internal policy controls and training, executive branch administrative oversight, enhanced congressional oversight, and civil and criminal penalties for abuse; and
- Finally, absolute statutory prohibition on the use of KD technology for non-terrorism investigations.

For more information, please see Paul Rosenzweig, “Proposals for Implementing the Terrorism Information Awareness System” at www.heritage.org/Research/HomelandDefense/lm8.cfm and Paul Rosenzweig and James X. Dempsey, “Technologies that Can Protect Privacy as Information Is Shared to Combat Terrorism” at <http://www.heritage.org/Research/HomelandDefense/lm11.cfm>.

Post Hearing Questions for the Record
"The Department of Homeland Security: The Road Ahead"
January 26, 2005
Submitted to Stephen E. Flynn, Ph.D.
From Senator Susan Collins

1. Given the wide range of activities over which the Department of Homeland Security has influence, is it essential that DHS coordinate its activities with other federal agencies. For example, bioterrorism responsibilities are divided between HHS and DHS. Do you think this division has worked to date, and if not, how do you think these responsibilities should be reallocated?

The inherently multi-jurisdictional, multi-disciplinary character of the homeland security mission, particularly when it comes to managing a bioterrorism incident, means that the Department of Homeland Security always will have to work closely and effectively with counterparts across the federal government and with local, state, and foreign governments. There are virtually no scenarios associated with the catastrophic terrorist threat that can be managed exclusively within the confines of DHS. This places a premium on coordination which requires adequate staffing, which DHS does not currently have, to maintain a full-time liaison with the relevant offices at HHS and the Centers for Disease Control (CDC). This liaison work should be a two-way street with senior personnel from HHS and CDC on permanent assignments at DHS to support their prevention and response activities. Also, in the event that a bioterrorist threat was directed at the nation's food supply vs. the general population, DHS needs to be able to coordinate closely with USDA, FDA, and the myriad state and local entities responsible for food safety. Since there is no CDC equivalent for managing disease outbreaks within the agricultural sector, a bioterrorist attack on the food supply system will pose a huge challenge for coordinating the response that the U.S. government is not currently positioned to meet.

2. Are there adequate plans to for the medical response to a bioterrorism attack, and are these plans the product of adequate coordination between DHS and HHS?

If a bioterrorism attack is quickly detected and the affected individuals are identified and contained at the locality of the incident, it likely that DHS and HHS will be able to marshal an effective response. However, none of the plans in place are adequate for dealing with a managing a major disease outbreak within the United States. This is so because of the paucity of public health capacity within states and localities, and the persistent commercial pressures within the private health care system to reduce the overhead costs associated with maintain capacity for which there is not routine demand. One particularly serious shortcoming is the inadequate planning and exercising at the local level for distributing national stockpiled medications. Delays associated with getting these medications to the affected population will translate into people developing symptoms and overwhelming the limited surge capacity that hospitals can provide, risking a collapse of the health care system just as the outbreak is getting started. A particularly daunting problem for which is there are currently no good plans, is how to

deal with the “worried-well” who present themselves for medical evaluation or treatment because they believe they might be experiencing symptoms associated with an epidemic. The best way to manage this risk is to get as much information as possible into the public domain before a disease outbreak so the general population can make informed individual judgments about whether they should present themselves for medical care. However, there has been a great deal of reluctance of undertaking such a public education campaign deriving from a concern over creating public anxiety.

3. During the 1990s, the Justice Department developed two different, incompatible fingerprint screening programs—IDENT was developed by the INS, and IAFIS was developed by the FBI. If has been a challenge for years to integrate these programs, a challenge made more difficult by moving the IDENT program over to DHS. The integration of these systems is critically important, especially given the fact that US-VISIT uses the IDENT system. Are these systems compatible, and if not, what it take to make them compatible?

I do not know enough about the technical details of these two programs to provide an informed response.

4. Can you comment on DHS's progress with the development and deployment of biometric identification systems in general and TWIC in particular? How do you view the priority they have given this program, more than three years after 9/11?

There are legitimate technical and privacy issues associated with the widespread deployment of biometric identification systems. As with many of the complex issues that confront the new Department of Homeland Security, they are not being addressed with the same level of urgency with which the U.S. government is adopting for dealing with the complex issues associated with the waging the war on terrorism abroad. Ultimately, establishing the sense of priority and marshalling the appropriate resources to resolve the legal and technical issues associated with the use of biometric identification systems must be set by the White House.

5. Can you discuss how DHS should ensure the interoperability and compatibility of the various biometric identification systems that have been deployed and are being developed by DHS and other agencies?

The President should ask the National Academies of Science to create a task force of the nation's leading experts on the development and deployment of biometric identification systems to evaluate the current efforts across the federal government to adopt these technologies and to propose a set of federal guidelines to govern their deployment.

6. In general, have DHS activities in the areas of technology development, preparedness, and intelligence been adequately coordinated with other federal agencies? If not, what recommendations would you make to improve this coordination?

No, DHS has not done an effective job at coordinating these activities with other federal departments and agencies. A central issue here is both the number and the composition of staffing assigned to DHS to manage these issues. Given the tremendous coordination challenges just with resolving longstanding conflicts and asymmetries associated with the capabilities among its legacy agencies, not surprisingly, much of the attention of the senior management at DHS has been inwardly focused. Since this senior management team is made up almost exclusively of (1) "detailees" drawn from and loyal to these agencies and (2) political appointees who possess limited experience with these issues and serve typically short tenures in government, DHS has been struggling with getting its own house in order. This has translated into a situation where there is only episodic outreach to other federal departments and agencies. To address this problem, DHS should borrow from the model of the Office of Secretary of Defense by building a cadre of non-political Senior Executive Service civilians to provide expertise and continuity for the department. Also, the other federal departments and agencies should be required to create well-staffed liaison offices at DHS to support these coordination efforts. This will require the White House and Congress to provide much more funding for personnel to manage DHS than they have shown an inclination to do to date.

Post Hearing Questions for the Record
“The Department of Homeland Security: The Road Ahead”
January 26, 2005
Submitted to Stephen E. Flynn, Ph.D.
From Senator Norm Coleman

1. In Fiscal Year 2004, St. Paul and Minneapolis received a total of \$20,108,247 in Urban Area Security Initiative Grants. However, this year St. Paul received no money and Minneapolis received only \$5,763,411. It seems to me that if we are to have a coherent homeland security strategy there needs to be consistency in the program, not only in terms of funding but in terms of rhyme and reason. Here you have two cities right next to each other that have an interconnected homeland security strategy. One was zeroed out altogether and apparently is to have no homeland security funding while the other was drastically cut. Doesn't a sound homeland security strategy depend on both consistency in terms of funding and policy to avoid wasting money and creating holes in our security?

The concerns you raise about funding for St. Paul and Minneapolis are symptomatic of a flawed approach to providing funding to state and local governments around the nation. One central issue is that advancing our national capacity to prevent and respond to incidents of catastrophic terrorism on U.S. soil rests primarily on the shoulders of local, county, and state shoulders. While there is a need to prioritize limited resources to the locations that are most likely to be attacked, or where the consequences and potential loss of life would be greatest should there be an attack, the federal government must identify minimum capabilities that each urban area should be maintaining to meet the homeland security imperative. Washington has been reluctant to set these minimum standards because of apprehension over the budgetary implications associated with helping jurisdictions to satisfy those standards. Instead, we have had the worst of all possible worlds: money distributed spasmodically and erratically, which makes it impossible for local and state government to undertake multiyear planning, particularly when it comes to hiring personnel.

2. I have been hearing from law enforcement personnel in Minnesota that the lines of communications between the Department of Homeland Security and local officials still need improvement. From your vantage point, what actions can the Department of Homeland Security take so that the lines of communication are improved and important information is passed along in a timely and effective manner?

The two most frequent complaints that I hear from law enforcement personnel around the nation is that they are not receiving sufficient “actionable” intelligence to guide their efforts, and that it is difficult to find the right person to talk at DHS when problems arise.

The first issue lies almost entirely outside DHS hands. The fact is that the federal government currently possesses very little useful intelligence to share. That being said,

the tendency at DHS to exercise extraordinary caution when sharing the limited information it has about vulnerabilities and terrorist activities with non-federal entities, or providing only information that has been so sanitized as to make it operationally meaningless, only fuels frustration and irritation at the state and local levels. DHS needs to err on the side of candor vs. caution since it will likely be the eyes and ears of local law enforcement that will make the difference in preventing the next act of terrorism.

The second issue speaks to the tremendous turnover at DHS which arises from the failure to provide adequate personnel billets and funding to adequately manage the department generally and to do liaison work at the state and local level specifically. DHS is populated with managers who are on temporary assignments from the agencies found within the department and political appointees who typically have only short tenures in working in the federal government.

3. With the emphasis on preparedness in current Department of Homeland Security and Office of Domestic Preparedness guidelines, do you think enough is being accomplished on the Prevention Front? What is your vision for state and local terrorism prevention efforts and how might you suggest dollars be allocated to meet that need?

Overall, there is not enough being done at the state and local levels to both prevent acts of terrorism or to respond to attacks when they inevitably occur. Part of the problem, is that operationally, the task of terrorism prevention cannot and should not be isolated from non-terrorist law enforcement and emergency preparedness activities. Everything we know about al Qaeda and its radical jihadist imitators is that they work hard to develop the means to blend into everyday life while they are preparing to carry out an attack. This means that it will be traditional police work that is most likely to spot their logistics and reconnaissance activities versus explicit counter-terrorist operations. That is, it is the authorities, presence, and relationships that local law enforcement maintains and exercises within its community that will best position it to detect and intercept terrorist activities. Similarly, the same people who are responsible for emergency planning and preparedness at the local level for non-terrorists incidents such as natural disasters are the same people a community is going to turn to in the aftermath of a terrorist attack to save lives and to restore critical systems. Accordingly, unless the federal government is willing to take a holistic approach to prevention and preparedness, state and local counter-terrorism efforts will be built on a fragile and unsupportable foundation.

4. With regard to student visas, several agencies are involved in determining which foreign students will be allowed to enter the United States to study. What is your view on how these agencies are cooperating with each other and do you think changes need to be made?

In general, I am of the view that one of the most potent anti-terrorism tools that the United States possesses is exposing young people from abroad to our society. We should be working hard to facilitate as many foreign students entering into our university systems as meet a given school's admissions standards while still checking to make sure that individuals with explicit terrorist links are not seeking to exploit the student visa

system to gain access to the United States. The most important improvement we could make is to adequately staff the agencies responsible for processing these applications so they can do so in an expeditious manner. There will never be much appetite for improving coordination when the student visa program is being run by harried government workers who start each day with an overflowing in-box.

5. Currently, when a foreign student wants to apply to school in the United States they need to pay a \$100 SEVIS fee before filling out a visa application. This is separate from the \$100 interview fee. If they are denied a visa, the \$100 SEVIS fee is not refunded. Also, when the student pays the SEVIS fee, they are entered into a database and their name is not removed if they are denied a visa. Do you think that the SEVIS fee process needs to be changed so foreign students are not deterred from applying for a visa and do you think the current management of the database needs to change so we do not have a database full of people that have never set foot on American soil?

Again, I think as a matter of policy, the U.S. government should be encouraging qualified foreign students to study in the United States. \$100 is a substantial sum of money, particularly for students from less developed nations. We should avoid the “penny-wise, pound-foolish” approach to imposing expensive fee-recovery requirements to finance the student visa programs. High costs will discourage the legitimate foreign students who we want to attract to the United States while being readily paid by any would-be terrorist who have ready access to the funding to gain entry into the country.

I do not know enough about the SEVIS database system to comment on the retention of names of those denied a visa.

6. I know that the State Department is working to reverse the decline in student visas. What role can and should the Department of Homeland Security play in reversing perceptions about America being unwelcome to foreign students?

Real improvements in managing the processing time for student visas and providing a well-funded ombudsmen program to resolve complaints when they arise will go a long way towards reversing this impression.

7. Currently border security officials located at the northern border of Minnesota and other states travel to facilities in Georgia for training. These sites are unable to provide training on how to handle the cold temperatures that border officials encounter on the Canadian border. Have you examined whether the Department of Homeland Security should consider adding training facilities in cold weather sites to better train border security personnel there?

No I have not. In general, as their jobs have become more complex and important to the security of the nation, there needs to be a far greater investment in training to support personnel assigned to DHS. If cold weather training were to be incorporated as a part of a broader initiative to improve the training infrastructure for the Customs and Border

Protection Agency, a case could certainly be made for building this in a northern state. However, building this facility solely for the purpose of providing cold weather training would not be the best use of resources, since this kind of training could be provided at a field-office level.

8. Recently HBO aired a film called "Dirty War" which described the chaos of a dirty bomb attack in downtown London. Although the film is set in England, could a dirty bomb attack or nuclear attack happen in the United States and are we prepared in the event it does happen?

An RDD attack almost certainly will happen in a major city of the United States in the next 10-15 years and an attack involving a nuclear weapon is possible. No major city in this country is prepared to deal with the aftermath of such an attack. Two specific shortcomings are the lack of public information about what citizens should do if they are exposed to this kind of an attack, and the absence of decontamination equipment to wash people and buildings down should they be exposed to radioactive materials.

Post Hearing Questions for the Record
"The Department of Homeland Security: The Road Ahead"
January 26, 2005
Submitted to Stephen E. Flynn, Ph.D.
From Senator Frank Lautenberg

1. The DHS Inspector General's office identified the port security grant program as lacking direction, or a priority basis on which to make grant awards. As a result of this, can you quantify the harm to the vulnerability of our nation's maritime system to terrorism? If not, what are the implications of a lack of clear security priorities for homeland security grant programs such as this?

The ports that should receive the highest priority are those that possess the most critical infrastructure, play the greatest role in a regional and national economy, and which are most proximate to major population centers. This criterion has not been used in guiding the port security grant programs. As a result, these ports remain very vulnerable to catastrophic terrorist attacks. There are currently no good studies to quantify the potential losses associated with a successful attack on seaports. Still, it should not require detailed scientific studies to inform a post-9/11 decision that the nation's largest ports should be the top priority when it comes to funding.

2. You mention the lack of training infrastructure at the Department. Can you identify personnel or offices within DHS that are in most need of further training or recommend further areas of investigation?

My biggest area of concern is the lack of training infrastructure to support the mission of the Customs of Border Protection Agency. With the new "one face at the border" program, former immigration agents are supposed to be in a position to detect violations of customs and animal and plant control laws while former customs agents are supposed to be in a position to detect violations of immigration laws. However, there are no new funds to provide these training opportunities within CBP. I also am concerned that the middle management in these agencies are not being afforded the kind of advanced education opportunities to support their increasingly complex and important missions. The Department of Defense should be asked to put together a training and education advisory task force to assess DHS's current and future training needs and to develop a proposal for meeting those needs.

3. While engaging the private sector in issues associated with critical infrastructure protection, I understand that the business cases aren't always present to support investment in homeland security improvements. What concrete measures can the Department take, or should Congress explore, to encourage proper investment? Are substantive standards necessary in each case? If should the IAOP continue to provide free security consulting services to the private sectors companies with no follow-up or required actions?

The market does not currently have sufficient incentives in place to work individually and collectively to secure critical infrastructure. For the last 20 years, these networks have been driven by four market imperatives: how to make them as *open* as possible; as *efficient* as possible; as *reliable* as possible; and their use as *low cost* as possible. Security has been viewed as raising costs, undermining efficiency, undermining reliability, and placing pressure to close the networks. As a result, we have networks that have extraordinary capacity to generate wealth but very little in the way of integrated security. Currently the architecture for the private / public sector interaction is largely static and ineffectual with the federal government sponsoring the development of what it determines to be “best practices” and exhorting the private sector to voluntarily adopt these practices. Since these practices carry with them new costs particularly when it comes to adding redundant capacity to make an infrastructure more resilient, private companies who are supportive of the measures always have to worry about the “free rider” problem; i.e., companies who choose to make a token or no effort to embrace the proposed security practices so that they can secure the short-term competitive advantage of not incurring the costs associated with making a good faith effort. Since security always involves a determination of “how much is enough?” companies also have to worry about the liability issue of having adopted practices which are judged in the aftermath of an event to have been insufficient. At the end of the day, what is required is highly selective and creative regulatory measures, modeled after some of the more effective environmental rules developed in the 1990s. Private sector entities should be directly involved in designing the optimal security measures, but the federal government must play a role in enforcing the standards and providing indemnification for those who embrace the standards, even if they subsequently prove insufficient to prevent a terrorist act.

4. On May 27, 2004, the FBI reportedly identified the stretch between Port Newark and Newark Liberty International Airport as the most dangerous two miles when it comes to terrorism. Do you agree with this assessment? Can you elaborate? Do you feel this security risk still exists?

This small area contains some of the most critical transportation, chemical, and energy links in the nation. As a result, an incident in any one of these sectors will likely have cascading effects across all the sectors. Given the concentration of maritime, rail, air, and highway infrastructure, and the dependency on the metropolitan New York area and New England on that transportation system, an attack on this region creates the risk of profound disruption to the entire northeast region of the United States. Still, despite the importance of this area, the modest new safeguards currently in place to protect, respond, and restore the critical networks are insufficient to deter a determined terrorist organization.

Post-Hearing Questions for the Record
 Submitted to Michael Wermuth
 From Senator Susan Collins

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

- Given the wide range of activities over which the Department of Homeland Security has influence, it is essential that DHS coordinate its activities with other federal agencies. For example, bioterrorism responsibilities are divided between HHS and DHS. Do you think this division has worked to date, and if not, how do you think these responsibilities should be reallocated?

In my view, the process has not worked satisfactorily. I will refer directly to text from the fourth “Gilmore Commission” report,¹ which fully articulates my own views:

“The *National Strategy for Homeland Security* has eliminated the distinction between ‘crisis’ and ‘consequence’ management. This will help remove certain ambiguities in the responsibilities and authority for planning and response. The creation of an overarching National Incident Response Plan to replace the Federal Response Plan and numerous other Federal plans can also clarify responsibilities. With the merger of the U.S. Customs Service (USCS), the U.S. Coast Guard (USCG), and the Immigration and Naturalization Service (INS)(and others) into the new DHS, that agency will have control over some but not all Federal law enforcement capability. The *National Strategy* provides that the Secretary of DHS will have the responsibility for ‘coordination and integration’ of Federal, State, local, and private’ activities for critical infrastructure protection (CIP). But it does not provide any vision about the extent to which DHS will be ‘in charge’ of executing a response during or after an attack on some CIP sector; nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks, especially a biological one.

“Recommendation: That the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies

“That situation is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, after DHS is formed, will be in charge in the event of a biological attack.

“Recommendation: That the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism attack, and specify its responsibilities and authority before, during, and after an attack; and designate the DHHS as the Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations”

¹ *IV. Implementing the National Strategy, Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (December 15, 2002), p.48. Available at: www.rand.org/nsrd/terrapanel

The commission made similar recommendations for DHS relationships with other federal departments and agencies (e.g., with USDA for agroterrorism-related activities). Such a process will require, at a minimum specific direction from the President, and could require legislation. Nevertheless, with any terrorist attack likely requiring resources and response activities from a variety of agencies, one should be "in charge." Because of its legislative mandate, its role as articulated in a series of Homeland Security Presidential Directives, and its responsibilities for coordinating the flow of information among entities at all levels, DHS should be given that mantle.

2. Are there adequate plans for the medical response to a bioterrorism attack, and are these plans the product of adequate coordination between DHS and HHS?

No. They are still major gaps in the substance of bioterrorism response plans and insufficient coordination between the departments.

3. During the 1990's, the Justice Department developed two different, incompatible fingerprint screening programs- IDENT was developed by the INS, and IAFIS was developed by the FBI. It has been a challenge for years to integrate these two programs, a challenge made more difficult by moving the IDENT program over to DHS. The integration of these systems is critically important, especially given the fact that US-VISIT uses the IDENT system. Are these systems compatible, and if not, what will it take to make them compatible?

I am not sure I agree that moving IDENT to DHS has made the challenge more difficult. Even when INS had the responsibility as a DOJ entity, its relationship with the FBI on such matters and others was no model for interagency coordination. Clearly, the systems are not currently directly compatible but work is being done to identify ways to make them so. Choices will have to be made after comparing both the effectiveness of integrating the two and the expense to do that, or requiring that one entity or another switch to the other's system.

4. Can you comment on DHS's progress with the development and deployment of biometric identification systems in general and TWIC in particular? How do you view the priority they have given this program, more than three years after 9/11?
5. Can you discuss how DHS should ensure the interoperability and compatibility of the various biometric identification systems that have been deployed and are being developed by DHS and other agencies?

ANSWERS TO QUESTIONS 4 AND 5:

Although we have not studied the DHS plans for biometric identification in a comprehensive way, including the specific details for development, deployment, interoperability, and compatibility, I will make a few observations from what I have

learned from a variety of sources, including news and other reports, discussions with DHS and other Executive Branch officials, and with RAND and other experts.

First, any positive personal identification involves major privacy and other significant policy implications. That includes especially the access to and proposed use of any data that may be derived from such systems. My observation from a distance is that DHS is very interested in the development of such systems but are to a certain extent constrained by such considerations—and they are important issues to be considered. To that extent, therefore, I do not fault DHS for the priority that they have placed on such development.

On the other hand, much still remains to be done in developing appropriate standards for such systems, that will include such considerations as near-zero false positive rates, real-time-verification and communications systems, assured compatibility and interoperability, and the necessary controls for privacy and other civil liberties implications. At present, about the only “standards” for such matters is what the (ever-increasing) vendors of such products may claim. That is not to say that there are not some using products already available, and “TWIC” cards could prove to be one method. It is not clear, however, the extent to which TWIC is compatible or interoperable with other systems.

Experience has shown that such compatibility and interoperability is essential in the electronic age and the ability to move rapidly to and from points almost anywhere in the world. To a certain extent, DHS has recognized that importance and is working to ensure that its IDENT program and the systems for US-VISIT are interoperable.

6. In general, have DHS activities in the areas of technology development, preparedness, and intelligence been adequately coordinated with other federal agencies? If not, what recommendations would you make to improve this coordination?

No, but not from lack of trying on DHS’s part. There are still many “turf” and agency “culture” issues to be overcome. These areas are some of those in which, as I described in my testimony, the White House must play a more robust role. DHS does not own everything related to technology development, preparedness, intelligence, and more.

For more discussion on these and related issues, I refer to the fifth “Gilmore Commission” report:

“We also recommend that the President establish an interagency mechanism for homeland security grants, led by the Secretary of DHS, to streamline and consolidate the grant application and decision process throughout the Federal government. The creation of such a process will reduce confusion among grant applicants and relieve them of some of the burden of multiple—and different—application processes. . . .

The sudden and large commitment of resources to a new mission carries with it some important challenges. Chief among these challenges is for DHS to

organize and coordinate an effective R&D program amid great uncertainty and across numerous operational needs. Moreover, DHS must contend with the challenges of implementing and coordinating research in an arena in which the organizations conducting research are almost entirely unrelated to the organizations that must implement the results of that research. Finally, DHS R&D efforts must be developed mindful of substantial fractions of both the research and user communities that are largely outside of the department.

Although DHS is given some R&D coordinating authority under the Homeland Security Act of 2002, that coordinating mechanism needs to be specified. **We recommend the formal establishment, by Executive Order or Presidential Decision Directive, of a Federal Interagency Homeland Security Research and Development Council, chaired by the Secretary of Homeland Security (or his designee) and with representatives of Federal R&D entities as well as end users.** Within that process, R&D should be categorized and prioritized across the entire Federal government, for internal (Federal laboratory) and external (contract and grant) programs. That process must also include input from end-users at the State and local levels, and from the private sector, both on requirements and on the utility of developed and emerging technologies. Moreover, that process must include procedures for establishing national standards for equipment and technology with government and private sector involvement.²

² *V. Forging America's New Normalcy, Fifth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (December 15, 2003), pp. 27 and 34. Available at: www.rand.org/nsrd/terrapanel

Post-Hearing Questions for the Record
Submitted to Michael Wermuth
From Senator Norm Coleman

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

1. In Fiscal Year 2004, St. Paul and Minneapolis received a total of \$20,108247 in Urban Area Security Initiative Grants. However, this year St. Paul received no money and Minneapolis received only \$5,763,411. It seems to me that if we are to have a coherent homeland security strategy there needs to be consistency in the program not only in terms of funding but in terms of rhyme and reason. Here you have two cities right next to each other that have an interconnected homeland security strategy. One was zeroed out altogether and apparently is to have no homeland security funding while the other was drastically cut. Doesn't a sound homeland security strategy depend on both consistency in terms of funding and policy to avoid wasting money and creating holes in our security?

I am no expert on the requirements, considerations, or processes for UASI grants. I do believe, however, that the program was not intended to provide a specific level of funding to designated cities year after year. It is my understanding that such funding has been intended as a “pump primer” to help cities overcome current shortfalls. According to DHS's own description:

The cities were chosen by applying a formula based upon a combination of factors including population density, critical infrastructure and threat/vulnerability assessment.³

Clearly, one or more of those factors can change from year to year. In addition, for grants in any year, a city must submit its own jurisdictional assessment, which includes its own statements of threats and vulnerabilities, and corresponding capabilities and needs. Without knowing the specifics of the Minneapolis-St. Paul situation, I can only surmise that, in applying various criteria and considering the justifications submitted, a determination was made that Minneapolis still had some shortfalls in requirements that justified additional funding in 2004 but that St. Paul did not. I also assume that such a determination does not preclude either city from applying for additional grants in the future, either from DHS or other federal agencies.

2. I have been hearing from law enforcement personnel in Minnesota that the lines of communication between the Department of Homeland Security and local officials still need improvement. From your vantage point, what actions can the Department of Homeland Security take so that the lines of communication are improved and important information is passed along in a timely and effective manner?

³ Accessed at <http://www.dhs.gov/dhspublic/display?theme=43&content=552&print=true>

In various contexts, we are hearing much the same thing. One of the great things about the way the United States is organized is our federal form of government, a strong national government for certain purposes and 50 sovereign states. For issues like these, that is also part of the bad news. DHS continues to struggle with how best to have that outreach when the several states and the thousands of local jurisdictions often have different ways of doing things, including both communications processes and requirements.

One good news story is the progress that has been made in developing the Homeland Security Information Network (HSIN)—especially the Joint Regional Information Exchange System (JRIES) now available in all 50 states and in dozens of major cities. More remains to be done, but there has been good progress in this area.⁴

3. With all the emphasis on preparedness in current Department of Homeland Security and Office of Domestic Preparedness guidelines, do you think enough is being accomplished on the Prevention Front? What is your vision for state and local terrorism prevention efforts and how might you suggest dollars be allocated to meet this need?

Clearly, there has, in recent years, been too much focus at the state and local levels on response and recovery activities. In part, that has arisen from the expectations that the federal government has been historically considered to have primacy over terrorism prevention activities.

There is, however, a growing realization among a number of state and local entities that the federal government cannot do everything in the prevention and that states and locals not only have some capabilities but, in fact, have some relevant experience that can be brought to bear.

Several jurisdictions have been setting the pace in this area and can and should serve as models for others. Notably are the States of California (with its California Anti-Terrorism Information Center⁵), and similar entities in Maryland and Virginia; the Los Angeles Operational Area Terrorism Early Warning Group (the model of which has now spread to numerous jurisdictions nationwide); and New York City, especially the programs of the NYPD.

I know from discussions with senior personnel in DHS that they will be increasing emphasis on funding and coordination for appropriate state and local prevention efforts.

Nevertheless, some are concerned and questioning to what extent local law enforcement should be engaged in activities that look more like intelligence

⁴ For more information on HSIN, see, e.g., http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0355.xml

⁵ See <http://caag.state.ca.us/antiterrorism/>

collection—"spying"—and what are the implications for such activities on civil liberties.⁶

4. With regard to student visas, several agencies are involved in determining which foreign students will be allowed to enter the United States to study. What is your view on how these agencies are cooperating with each other and do you think changes need to be made?

It would appear that that process has improved dramatically just in recent days.⁷

5. Currently, when a foreign student wants to apply to school in the United States they need to pay a \$100 SEVIS fee before filling out a visa application. This is separate from the \$100 interview fee. If they are denied a visa, the \$100 SEVIS fee is not refunded. Also, when the student pays the SEVIS fee, they are entered into a database and their name is not removed if they are denied a visa. Do you think that the SEVIS fee process needs to be changed so foreign students are not deterred from applying for a visa and do you think the current management of the database needs to change so we do not have a database full of people that have never set foot on American soil?

I am a firm believer in fee-based services. I can think of no better way to help fund a program like SEVIS than to charge a fee. Respectfully, it does not bother me at all that a fee is not returned if a visa is denied. Nor am I concerned that we develop data and persons who are legitimately denied entry into the United States. It is, of course, a matter of continuing concern how such data will be used, who has access to it, and on what basis it is audited, corrected, and updated.

The fifth report of the "Gilmore Commission" contained the following discussion and recommendation (a similar recommendation was made seven months later by the 9-11 Commission):

An on-going debate exists in the United States about the tradeoffs between security and civil liberties. History teaches, however, that the debate about finding the right "balance" between security and civil liberties is misleading. This traditional debate implies that security and liberty are competing values and are mutually exclusive. It assumes that our liberties make us vulnerable and if we will give up some of these liberties, at least temporarily, we will be more secure. Yet, consider the context in which civil liberties were first firmly established. The framers of the Constitution had just survived a true threat to their existence and were acutely aware of the fragility of their nascent nation. In this uncertain and insecure environment, the framers chose not to consolidate power and restrict freedoms but to devolve power to the people and protect civil liberties from encroachment. They recognized that civil liberties and security are mutually reinforcing.

⁶ Cf. <http://www.aclu-or.org/issues/terrorism/181/181challenges.html>;
http://www.commandcollege.com/futures_files/abstracts/000003dc.htm;
<http://www.csindy.com/csindy/2003-12-04/news3.html>

⁷ See <http://www.washingtonpost.com/wp-dyn/articles/A56612-2005Feb26.html>

The Declaration of Independence has at its core the premise that there are certain "unalienable Rights, that among these are Life, Liberty and the Pursuit of Happiness." What terrorists seek to destroy requires a comprehensive strategy to defeat their objectives, while preserving not only life but also liberty and our uniquely American way of life.

We must, therefore, evaluate each initiative along with the combined effect of *all* initiatives to combat terrorism in terms of how well they preserve all of the "unalienable rights" that the founders believed were essential to the strength and security of our nation—rights that have become so imbedded in our society and ingrained in our psyche that we must take special precautions, take extra steps, to ensure that we do not cross the line. It is more than the clearly defined protections in the Constitution—protections against unreasonable search and seizure; and against self-incrimination. It is also that less well-defined but nevertheless exceptionally important "right to privacy" that we have come to expect and that our judicial system has come increasingly to recognize.

As an example, we should not move away from the traditional requirement for a criminal predicate to justify law enforcement activity. As a nation, our most significant concerns with broadening law enforcement powers should be

- the potential chilling effect of allowing the monitoring of First Amendment activities, such as freedom to peaceably assemble, the free exercise of religion, and freedom of speech, to the point where it discourages the exercise of or directly impinges on these fundamental rights; and
- the increasing reliance on more sophisticated technology that has vast potential for invading our privacy.

Military intelligence gathering as an aid to law enforcement or as part of military "homeland defense" missions was not fully anticipated by our existing system of laws and safeguards. It now becomes essential for the Congress to legislate and for the Department of Defense to implement through clear procedures the limitations on the use of satellite imagery and other advanced technology monitoring inside the United States. Such limitations, we suggest, should be similar to those governing electronic surveillance for intelligence purposes inside the United States under the Foreign Intelligence Surveillance Act of 1978.

To enhance both our security and our liberty, we recommend that the President establish an independent, bipartisan civil liberties oversight board to provide advice on any change to statutory or regulatory authority or implementing procedures for combating terrorism that has or may have civil liberties implications (even from unintended consequences).⁸

6. I know that the State Department is working to reverse the decline in student visas. What role can and should the Department of Homeland Security play in reversing perceptions about America being unwelcome to foreign students?

The State Department should have the primary role in "reversing perceptions"—that being essentially a diplomatic matter—and progress is being made (see the answer to 4., above). The most appropriate role for DHS is to cooperate fully with State and to be transparently *seen* as cooperating.

⁸ Op. cit. pp. 22-23

7. Currently border security officials located at the northern border of Minnesota and other states have to travel to facilities in Georgia for training. These sites are unable to provide training on how to handle the cold temperatures that border officials encounter on the Canadian border. Have any of you examined whether the Department of Homeland Security should consider adding training facilities in cold weather sites to better train border security personnel there?

We have not looked at that issue directly, nor am I familiar with any other entities that may have studied that particular problem.

Post-Hearing Questions for the Record
Submitted to Richard Falkenrath, Ph.D.
From Senator Susan Collins

“The Department of Homeland Security: The Road Ahead”

January 26, 2005

- 1. Given the wide range of activities over which the Department of Homeland Security has influence, it is essential that DHS coordinate its activities with other federal agencies. For example, bioterrorism responsibilities are divided between HHS and DHS. Do you think this division has worked to date, and if not, how do you think these responsibilities should be reallocated?**

The question is very difficult to answer in general. As you note, homeland security is not the exclusive domain of any one department or agency, even if the Department of Homeland Security has a majority to the U.S. homeland security budget. Interagency coordination is vitally important – and extraordinarily difficult. Interagency coordination is generally the responsibility to the White House staff, which since October 8, 2001, has had a small staff within the White House Office dedicated to homeland security coordination and policy development. This is where I worked until May 2004.

I believe that reallocating the responsibilities of the various federal departments and agencies should generally be viewed as a last resort in addressing interagency coordination problems. The first resort should be improved central coordination by the responsible White House staff – a function that needs to be exercised from the highest levels of the government down to the middling levels, and which concerns operations as well as policy. A competent White House staff, properly empowered by the President, should be able to resolve most problems of interagency coordination.

I am particularly concerned about are a number of seams in division of homeland security responsibilities among various federal departments and agencies. Civilian biodefense, which you mentioned, is a particularly difficult area. The seam between the FBI and ICE in the area of domestic investigation is another, as is the three-way split between DHS, State, and Justice/FBI on matters of alien admittance and removal. These are the areas that require particularly close attention by responsible White House staff.

- 2. Are there adequate plans for the medical response to a bioterrorism attack, and are these plans the product of adequate coordination between DHS and HHS?**

I do not believe that the government possesses adequate plans or capabilities for dealing with the medical consequences of a high-end bioterrorism attack. The reliance on non-accountable and often unengaged state and local health agencies for key aspects of the plans is a particular problem,

and is the absence of an adequate legal framework for the administration of medical countermeasures during a bioterrorist threat or attack.

HHS has led the U.S. civilian biodefense effort. When it was first created, DHS was endowed with relatively little expertise or capability in this area. Development of such biodefense expertise and capability has not been a high priority for the Department to date. I believe the cooperation between the two departments could and should be substantially enhanced, but DHS will need to develop greater internal expertise if this collaboration is going to be a fruitful one.

3. **During the 1990s, the Justice Department developed two different, incompatible fingerprint screening programs – IDENT was developed by the INS, and IAFIS was developed by the FBI. It has been a challenge for years to integrate these programs, a challenge made more difficult by moving the IDENT program over to DHS. The integration of these systems is critically important, especially given the fact that US-VISIT uses the IDENT system. Are these systems compatible, and if not, what will it take to make them compatible?**

I agree completely with the premise of your question. The existence of two separate fingerprint systems is an embarrassment, a security weakness, and a source of enormous inefficiency in our law enforcement and homeland security systems. It is appalling that the Justice Department and the Congress allowed these two systems to be separately developed in 1990s.

The systems are not compatible. IDENT, the basis for the U.S. Visit program, used only two fingerprints. IAFIS, a far more robust system, uses 10.

I believe that IAFIS should become the central and sole federal repository of fingerprint data. IAFIS should, in effect, become a service provider to multiple different users in the federal government (e.g., VISIT, DOD fingerprinting of detainees, law enforcement bookings, credentials, etc.) as well as private, state, local, and international users, as appropriate. The separate fingerprint database in IDENT/VISIT should be moved into the IAFIS architecture. VISIT should transition from two to ten fingerprints, and should perform real-time checks against the IAFIS database. All fingerprint data taken at U.S. points of entry under the VISIT program should be permanently added to the IAFIS database.

4. **Can you comment on DHS's progress with the development and deployment of biometric identification systems in general and TWIC in particular? How do you view the priority they have given this program, more than three years after 9/11 ?**

As the previous question about IAFIS and IDENT makes clear, biometric identification systems cannot and should not be the sole responsibility of any single department or agencies. Whenever any one agencies seeks to develop its own separate identification standard for whatever particular function it is working on at the time, inefficiency and ineffectiveness down the line is virtually guaranteed.

The federal government's approach to identification standards and credentials, including biometrics, has been far too fragmented and to a certain extent remains so. This is not the fault of any one particular department or agency but of the Administration as a whole. Homeland Security Presidential Directive 12 ("Policy for a Common Identification Standard for Federal Employees and Contractors"), is a step in the right direction, but does not go far enough. The standard directed by the President should apply not just to U.S. government identification documents for federal employees but should be suitable for any identification application and should be required by the government at all federally-controlled access points, including points of entry into the country. Among other things, this would make clear that the standard would apply to passports issued by the United States and foreign countries, and that the standard could apply to drivers licenses.

The TWIC program is anachronistic. It makes no sense to have a separate identification program just for transportation workers. The program should be incorporated into the larger framework made possible by HSPD-12.

5. Can you discuss how DHS should ensure the interoperability and compatibility of the various biometric identification systems that have been deployed and are being developed by DHS and other agencies?

This task is beyond the capacity of DHS. DHS cannot issue orders or control the operations of other executive departments and agencies. Only a statute or, if no prohibited by statute, the President (or, in certain limited exceptions, the Chief of Staff or the Director of the Office of Management and Budget) can do this.

6. In general, have DHS activities in the areas of technology development, preparedness, and intelligence been adequately coordinated with other federal agencies? If not, what recommendations would you make to improve this coordination?

I do not have a general answer to this question. Since DHS activities are well coordinated, some or not. The extent of interagency coordination is usually determined by the personalities and backgrounds of the individuals involved, the histories of the offices involved, and the extent and vigor of White House intervention. Statutory requirements are not effective instruments for promoting interagency coordination.

Similarly, the multitude of Congressional committees and subcommittees with oversight responsibilities in the homeland security areas actually works against interagency coordination, since the various offices involved almost always have different Congressional patrons.

Post-Hearing Questions for the Record
Submitted to Richard Falkenrath, Ph.D.
From Senator Norm Coleman

"The Department of Homeland Security: The Road Ahead"

January 26, 2005

1. In Fiscal Year 2004, St. Paul and Minneapolis received a total of \$20,108,247 in Urban Area Security Initiative Grants. However, this year St. Paul received no money and Minneapolis received only \$5,763,411. It seems to me that if we are to have a coherent homeland security strategy there needs to be consistency in the program not only in terms of funding but in terms of rhyme and reason. Here you have two cities right next to each other that have an interconnected homeland security strategy. One was zeroed out altogether and apparently is to have no homeland security funding while the other was drastically cut. Doesn't a sound homeland security strategy depend on both consistency in terms of funding and policy to avoid wasting money and creating holes in our security?

I am unaware of the particular factors which determined the UASI grants to St. Paul and Minneapolis in FY04 and FY05, respectively. Any number of different factors – some sensible, some not – could have led to this outcome. Perhaps St. Paul had large unexpended balances from FY04, for instance. I do not know.

Determining homeland security grant levels to various state and local entities have been one of the most vexing questions facing the Administration since 9/11. There is no way to make all the people happy all the time, and nationwide there are countless seemingly illogical local outcomes such as the one you described in your question. The Administration approach, which I continue to believe is correct, has been to seek to rely the 50 governors to determine precisely how and where to distribute grant moneys within states. This approach is based on the belief that it is simply impossible for the federal government to coherently and effectively manage separate grants to the tens of thousands of state and local agencies across the country that play a role in homeland security. The Administration's hope had been that the governors offices' would play a helpful role in developing statewide plans for capacity building. This hope has frequently been disappointed.

2. I have been hearing from law enforcement personnel in Minnesota that the lines of communication between the Department of Homeland Security and local officials still need improvement. From your vantage point, what actions can the Department of Homeland Security take so that the lines of communication are improved and important information is passed along in a timely and effective manner?

In general, I believe the Department of Homeland Security does a pretty good job communicating with law enforcement and other public safety personnel. Indeed, from my position at the White House, I often felt that the Department was putting out too much information to state, local, and private sector officials, not too little. Within the government, DHS is a powerful advocate for sharing information with responsible state, local, and private sector officials.

DHS's communication with non-federal public safety personnel needs to be coordinated with the federal interagency. I believe that the procedures for doing this are generally effective and quick. Further, I think it is extremely valuable that DHS and the FBI have begun to issue just bulletins and advisories, which reduces confusing among non-federal law enforcement agencies.

3. With all the emphasis on preparedness in current Department of Homeland Security and Office of Domestic Preparedness guidelines, do you think enough is being accomplished on the Prevention Front? What is your vision for state and local terrorism prevention efforts and how might you suggest dollars be allocated to meet this need?

I believe that prevention should be our highest priority, higher certainly than preparedness and response. Most of our preventative initiatives are focused on federal agencies and capabilities. With the exception of the Joint Terrorism Task Forces, which I think work well, the federal government has not yet devised a strategy for fully exploiting and augmenting the capabilities of state, local, and private-sector entities with respect to the prevention of terrorist attacks.

4. With regard to student visas, several agencies are involved in determining which foreign students will be allowed to enter the United States to study. What is your view on how these agencies are cooperating with each other and do you think changes need to be made?

My understanding is that the Homeland Security Act of 2002 centralized in the Secretary of Homeland Security almost all authority over the admittance of foreign nationals into the United States. I am unaware of any other department or agency with the statutory authority to determine which foreign students will be allowed to enter the United States to study.

5. Currently, when a foreign student wants to apply to school in the United States they need to pay a \$100 SEVIS fee before filling out a visa application. This is separate from the \$100 interview fee. If they are denied a visa, the \$100 SEVIS fee is not refunded. Also, when the student pays the SEVIS fee, they are entered into a database and their name is not removed if they are denied a visa. Do you think that the SEVIS fee process needs to be changed so foreign students are not deterred from applying for a visa and do you think the current management of the database needs to change so we do not have a database full of people that have never set foot on American soil?

I would support eliminating all fees for foreign students applying to study in the United States as a means of promoting foreign student interest and enrollment. Fees for other kinds of visas should be increased to make up for the lost revenue on student visas.

6. I know that the State Department is working to reverse the decline in student visas. What role can and should the Department of Homeland Security play in reversing perceptions about America being unwelcome to foreign students?

The Department of Homeland Security needs to work to reverse the reality of America being unwelcome to foreign students by lowering the cost of student visa fees and making other reforms, as appropriate. The Department of State is responsible for U.S. public diplomacy abroad, and it needs to take responsibility for reversing foreign perceptions about America being unwelcome to foreign students.

7. Currently border security officials located at the northern border of Minnesota and other states have to travel to facilities in Georgia for training. These sites are unable to provide training on how to handle the cold temperatures that border officials encounter on the Canadian border. Have any of you examined whether the Department of Homeland Security should consider adding training facilities in cold weather sites to better train border security personnel there?

It would hope that some agency in the U.S. government already has a training facilities in a cold weather sites. Rather than DHS building a new facility to meet this need, it seems to me that the Federal Law Enforcement Training Center (FLETC) in Georgia should work out a cooperative arrangement for extramural cold-weather training of border security personnel.

